TASK ORDER

GSQ0015AJ0022

GSA Enterprise Operations (GEO)

in support of:

General Services Administration Information Technology (GSA IT)

Issued to:
Science Applications International Corporation

Under:
GSA Alliant Governmentwide Acquisition Contract

DUNS #078883327
Alliant Contract # GS00Q09BGD0048

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405

September 2015

FEDSIM Project Number 15010GSM

NOTE: The Section numbers in this Task Order (TO) correspond to the Section numbers in the Alliant Contract.

B.1 GENERAL

The work shall be performed in accordance with all Sections of this TO and the contractor's Basic Contract, under which the resulting TO will be placed. An acronym listing to support this Task Order Request (TOR) is included in Section J, Attachment H.

B.5 CONTRACT ACCESS FEE

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a Contract Access Fee (CAF). The amount of the CAF is ¾ % (i.e., (.0075)) of the total price/cost of contractor performance. This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO award. CAF is capped at $100,000.00 per contract year.

B.6 ORDER TYPES

The contractor shall perform the effort required by this TO on a Cost-Plus-Award-Fee (CPAF) basis for CLINs 0001, 1001, 2001, 3001, 4001, 0002, 1002, 2002, 3002, 4002, 0003, 1003, 2003, 3003, and 4003 and Not-to-Exceed (NTE) for CLINs: 0004, 1004, 2004, 3004, 4004, 0005, 1005, 2005, 3005, 4005 , 0006, 1006, 2006, 3006, 4006, 0007, 1007, 2007, 3007, and 4007.

B.7 ORDER PRICING (ALL ORDER TYPES)

Long distance travel is defined as travel over 50 miles from the primary duty stations listed in section F.4. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CLIN	Contract Line Item Number
CPAF	Cost-Plus-Award-Fee
NTE	Not-to-Exceed
ODC	Other Direct Cost

B.7.1.1 BASE PERIOD:

MANDATORY LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
0001	Task 1: Program Management	(b) (4)		
0002	Tasks 2 - 5			

OPTIONAL LABOR CLIN

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
0003	Task 6: Provide Enterprise IT Infrastructure As-Needed Capabilities - Surge	(b) (4)		

COST REIMBURSEMENT TRAVEL, TOOLS, and ODCs CLINs

CLIN	Description		Total Ceiling Price
0004	Long Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
0005	Tools Including Indirect Handling Rate (b) (4)	NTE	
0006	ODCs Including Indirect Handling Rate (b) (4)	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
0007	Contract Access Fee	NTE	(b) (4)

TOTAL CEILING BASE PERIOD CLINs: $102,696,093

B.7.1.2 FIRST OPTION PERIOD:

MANDATORY LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
1001	Task 1: Program Management	(b) (4)		
1002	Tasks 2 - 5			

OPTIONAL LABOR CLIN

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
1003	Task 6: Provide Enterprise IT Infrastructure As-Needed Capabilities - Surge	(b) (4)		

COST REIMBURSEMENT TRAVEL, TOOLS, and ODCs CLINs

CLIN	Description		Total Ceiling Price
1004	Long Distance Travel Including Indirect Handling Rate _(b) (4)	NTE	(b) (4)
1005	Tools Including Indirect Handling Rate _(b) (4) %	NTE	
1006	ODCs Including Indirect Handling Rate (b) (4)	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
1007	Contract Access Fee	NTE	(b) (4)

TOTAL CEILING FIRST OPTION PERIOD CLINs: $114,147,232

B.7.1.3 SECOND OPTION PERIOD:

MANDATORY LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
2001	Task 1: Program Management	(b) (4)		
2002	Tasks 2 - 5			

OPTIONAL LABOR CLIN

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
2003	Task 6: Provide Enterprise IT Infrastructure As-Needed Capabilities - Surge	(b) (4)		

COST REIMBURSEMENT TRAVEL, TOOLS, and ODCs CLINs

CLIN	Description		Total Ceiling Price
2004	Long Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
2005	Tools Including Indirect Handling Rate (b) (4)	NTE	
2006	ODCs Including Indirect Handling Rate (b) (4)	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
2007	Contract Access Fee	NTE	(b) (4)

TOTAL CEILING SECOND OPTION PERIOD CLINs: $111,789,698

B.7.1.4 THIRD OPTION PERIOD:

MANDATORY LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
3001	Task 1: Program Management	(b) (4)		
3002	Tasks 2 - 5			

OPTIONAL LABOR CLIN

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
3003	Task 6: Provide Enterprise IT Infrastructure As-Needed Capabilities - Surge	(b) (4)		

COST REIMBURSEMENT TRAVEL, TOOLS, and ODCs CLINs

CLIN	Description		Total Ceiling Price
3004	Long Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
3005	Tools Including Indirect Handling Rate (b) (4)	NTE	
3006	ODCs Including Indirect Handling Rate (b) (4)	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
3007	Contract Access Fee	NTE	(b) (4)

TOTAL CEILING THIRD OPTION PERIOD CLINs: $110,548,230

B.7.1.5 FOURTH OPTION PERIOD:

MANDATORY LABOR CLINS

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
4001	Task 1: Program Management	(b) (4)		
4002	Tasks 2 - 5			

OPTIONAL LABOR CLIN

CLIN	Description	Cost	Award Fee	Total Cost Plus Award Fee
4003	Task 6: Provide Enterprise IT Infrastructure As-Needed Capabilities - Surge	(b) (4)		

COST REIMBURSEMENT TRAVEL, TOOLS, and ODCs CLINs

CLIN	Description		Total Ceiling Price
4004	Long Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
4005	Tools Including Indirect Handling Rate (b) (4)	NTE	
4006	ODCs Including Indirect Handling Rate (b) (4)	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
4007	Contract Access Fee	NTE	(b) (4)

TOTAL CEILING FOURTH OPTION PERIOD CLINs: $110,773,239

GRAND TOTAL CEILING ALL CLINs: $549,954,492

B.12 SECTION B TABLES

B.12.1 INDIRECT/MATERIAL HANDLING RATE

Long Distance Travel, Tools, and ODC costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's disclosed practices.

- If no indirect/material handling rate is allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.
- If no rate is specified in the basic contract, no indirect rate shall be applied to or reimbursed on these costs.
- If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs.

The indirect handling rate over the term of the task order shall not exceed the rate specified in the schedule of prices above.

B.12.2 DIRECT LABOR RATES

Labor categories proposed shall be mapped to existing Alliant labor categories.

B.13 INCREMENTAL FUNDING

B.13.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding in the amount of (b) (4) for **CLINs 0001-0007** is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs will be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through the end of the Base Year of performance, unless otherwise noted in Section B.X. The TO will be modified to add funds incrementally up to the maximum of (b) (4) over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

Incremental Funding Chart for CPAF (Attachment S)

See Section J, (Attachment S) - Incremental Funding Chart (Excel Spreadsheet).

Attachment to be provided upon award.

B.14 AWARD FEE PLANNED VALUE/RESULTS REPORTING TABLE

The Award Fee Determination Plan (AFDP) establishes award fee. See Section J, Attachment G – Award Fee Determination Plan (Word document). The Award Fee Planned Value/Results Table to be provided upon award.

C.1 BACKGROUND

The General Services Administration (GSA) mission is to deliver best value in real estate, acquisition, and technology services to Government and the American people.

The scope of the work at GSA is vast and varied, but the mission is simple and to the point. GSA serves the Government and the American people. Through implementing its mission, GSA aspires to achieve three strategic goals:

a. *Savings*—provide savings to Federal departments and agencies. GSA uses purchasing power and expertise to deliver cost-effective real estate, acquisition, and technology solutions to Federal departments and agencies.
b. *Efficiency*—improve the efficiency of operations and service delivery. GSA will streamline operations to offer high-quality real estate, acquisition, and technology services at a good value to Federal departments and agencies.
c. *Service*—deliver excellent customer service. GSA will deliver excellent customer service to Federal agencies and departments by making it easier to do business with GSA.

GSA Information Technology (IT) supports the agency's strategic goals—savings, efficiency, and service—and enables excellence in the business of Government. GSA IT takes pride in delivering first-class products and services to its customers, and continues to strive to be a best-in-class IT organization for the Federal Government. GSA IT delivers enterprise IT services to end users within GSA, enables business portfolios by providing high-quality IT solutions to meet business needs, manages business relationships, and provides governance to develop and execute the GSA IT mission.

C.1.1 PURPOSE

GSA IT requires assistance with managing and evolving IT Service Delivery for the GSA Enterprise. GSA IT requires an Information Technology Infrastructure Library (ITIL)-based solution that has an integrated, enterprise-wide focus to deliver shared IT services in accordance with GSA IT's governance structure and portfolio-based framework.

C.1.2 AGENCY MISSION

GSA IT provides enterprise-wide IT service delivery and management to its large, diverse, and mobile customer base worldwide. GSA IT focuses on delivering innovative, mobile-ready, and collaborative solutions for its users and strives to be the technology leader in agility, efficiency, mobility, and productivity. GSA IT provides:

a. Enterprise-wide IT infrastructure services, including desktop support and wide area networking.
b. IT portfolio management (capital planning and investment control).
c. IT security programs and security management.
d. Enterprise architecture to support and link GSA business needs to IT systems and services.

e. Enterprise applications for email, collaboration, and identity management.

The following GSA IT principles guide the overall operations for the unified organization:

a. *Service-delivery mindset:* GSA IT delivers high-quality and reliable IT services to its customers.
b. *Adaptable organization:* GSA IT quickly and effectively responds to business priorities.
c. *Technology mastery:* GSA IT has the business and IT skills to apply the right technologies to solve business challenges in the most cost-effective manner.
d. *Governance and data-driven decisions:* GSA IT makes data-driven decisions using an enterprise governance framework.
e. *Standardization and continuous improvement:* GSA IT implements mature processes and standards that are maintained through feedback mechanisms.
f. *People-centric focus:* GSA IT invests in its people.

C.2 SCOPE

The scope of this Task Order (TO) includes delivering, managing, and evolving IT Services for the entire GSA Enterprise and entities as listed in Section J, Attachment N. The GSA Enterprise consists of over 16,500 direct users located in over 700 Continental United States (CONUS) and Outside the Continental United States (OCONUS) locations. GSA's current customer location and user counts can be seen in Section J, Attachment L. GSA requires an ITIL-based, flexible, highly integrated and increasingly cloud- and portfolio-based solution. This solution will support a mobile workforce and deliver productivity enhancing IT services to those workers anywhere, at any time, and on any device. The major task areas are defined below:

TASK 1: Provide Program Management

TASK 2 – Provide Service Strategy

TASK 3 – Provide Service Design

TASK 4 – Provide Service Transition

TASK 5 – Provide Service Operations

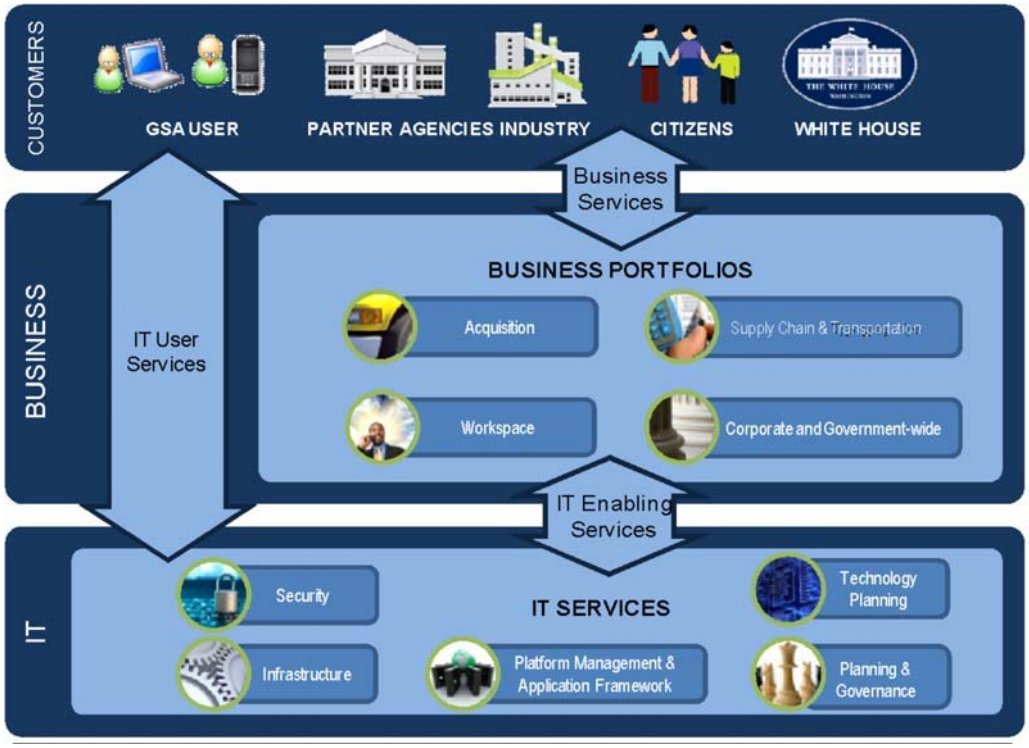
TASK 6 – Enterprise IT Infrastructure As-Needed Capabilities- Surge

C.3 CURRENT INFORMATION TECHNOLOGY IT ENVIRONMENT

The strategic GSA IT direction, as a result of a recent consolidation within GSA, will shift IT delivery from a decentralized, stove-piped approach to a business model that has an integrated, enterprise-wide focus. This model employs a portfolio-based approach that delivers shared services using an established governance structure as discussed in the GSA IT Information Resource Management (IRM) Strategic Plan (Section J, Attachment M).

GSA IT is currently aligning its IT capabilities by business portfolio or IT service to enable GSA IT to meet cross-agency needs in its service delivery. GSA has four business portfolios and five IT services, as described below. The business portfolios support the agency's business and applications, while the IT services deliver specific, consolidated, enterprise IT services and capabilities required by GSA. With this portfolio-based approach, GSA IT expects to realize cost

savings and increase operational efficiency in delivering IT services to both GSA internal and external customers. With this portfolio-based approach, GSA IT will better serve its customers.



The current portfolios and services are as follows:

a. *Workspaces Portfolio:* This portfolio provides fiscal management, process management, and engineering management for construction management, space delivery, facilities management, real asset management, and real property acquisition and disposal.

b. *Supply Chain and Transportation Portfolio:* This portfolio supports supply chain, travel, transportation, and card services management.

c. *Acquisition Portfolio:* This portfolio identifies key functions and applications supporting the entire acquisition life cycle for GSA. Key functions include requirements definition, acquisition planning and market research, synopsis and solicitation, source selection, award, contract administration and performance monitoring, and contract closeout.

d. *Corporate and Government-wide Portfolio:* This portfolio supports information reporting and dissemination, collaboration and education, policy-enabling systems, policy implementation, and human resources and financial management functions.

e. *Security Service:* This service supports business systems and end users, and it enables GSA to meet its mission and business objectives by implementing a high-performance, risk-based security program and organization for information and information system security management.

f. *Infrastructure Service:* This service manages, maintains, and supports enterprise infrastructure and GSA systems and websites.

g. *Platform Management and Application Framework Service:* This service standardizes GSA technology platforms and provides an application framework that is shared across the agency.
h. *Planning and Governance Service:* This service provides a structure to align IT strategy with business strategy, ensuring that GSA IT organizations stay on track to achieve our strategies and goals, and implements an effective means of measuring IT performance.
i. *Technology Planning Service:* The focus of this service is requirements management, data management, and program management. By adopting common data standards and a data model, identifying requirements at an appropriate level, and providing ongoing program reviews, GSA IT will reduce data redundancy, improve data accessibility, and ensure programs are effectively implemented.

On the basis of the needs of the GSA IT stakeholders and agency goals, GSA IT has established strategic commitments for fiscal years (FYs) 2014–2018. These commitments will provide a framework and guide the Enterprise Service Delivery and Management services provided under this TO and are further defined below:

a. *Commitment 1: Streamline IT Infrastructure Operations* - Improve operational efficiency by streamlining processes, standardizing technology usage, and utilizing commodity IT and shared services.
b. *Commitment 2: Maintain a Secure IT Environment* - Provide efficient GSA IT security, compliance, and privacy program capabilities that are sustainable, scalable, and flexible in order to support the compliance, operational, and business needs of the enterprise.
c. *Commitment 3: Improve Financial Management of IT Resources* - Improve financial performance by implementing effective governance processes and data-driven decisions to reduce IT costs and to better apportion the total IT spend.
d. *Commitment 4: Drive Accurate Business Analytics* - Provide innovative technology solutions to make quality data readily available and to translate data into useful information for strategic decision making.
e. *Commitment 5: Improve Business Applications/Systems* - Implement intuitive, integrated, and easy-to-train-on IT solutions based on the business direction in a less complex and streamlined IT environment.
f. *Commitment 6: Consolidate IT Service Delivery Across GSA* - Increase customer satisfaction by delivering IT services through the use of cost-effective technology solutions and a governance framework to satisfy the needs of internal and external business partners.
g. *Commitment 7: Use Innovation to Modernize the IT Environment* - Implement IT to drive the way GSA operates and does business with its partners and customers to generate business value and revenue.
h. *Commitment 8: Recruit and Empower a Competent, Diverse IT Workforce* - Recruit, empower, and support a high-performing, competent, and diverse IT workforce that combines business know-how and technology expertise to deliver exceptional IT services.

C.4 TASK ORDER OBJECTIVES

GSA IT has set the following TO objectives for the execution of GEO:

a. Deliver IT services that are well-integrated, flexible, and adaptable across all IT service areas, with the ability to rapidly scale in response to GSA's dynamic business environment.

b. Transform to an ITIL-based service delivery model and provide contiguous end-to-end service delivery with a single point of contact (cradle-to-grave) for IT support services from deployment through problem resolution and technology replacement.

c. Support a highly mobile workforce and deploy greater coverage at remote sites to increase the use of real-time and team-based collaboration tools. GSA seeks to modernize its network infrastructure by providing field offices with upgraded network connectivity. Most field office locations have T1 circuits today.

d. Develop a balance between delivering tactical support (operations and maintenance) and strategic support (development, modernization, and enhancement) that achieves operational and cost efficiencies while positioning stakeholders and their respective business lines to fulfill their missions.

e. Deploy IT services appropriately to the identified need with the ability to apportion charges to internal and external clients according to use. (A functioning equitable and transparent service charge back mechanism in place across the enterprise.)

f. Maintain a secure environment that includes necessary authorization and authentication, which adequately protects privacy information.

g. Support GSA's infrastructure strategy of providing "Anytime, Anywhere, Any Device" support. Key elements of this strategy are:

    1. Desktop/Server Virtualization - Any Device: Browser Based, Decreased Network Load, Easier Support Model, Reduced Cost.
    2. Cloud Email and Storage - Anytime, Anywhere, Any Device: Google Docs, User Data, Unlimited Capacity.
    3. Network Optimization - Anywhere: Secure, Full Fidelity User Experience in Headquarters (HQ), Regional Office Buildings (ROB), Field Offices, and Internet.
    4. Service Availability - Anytime: Resilient Systems, Data Center Consolidation and Replication, Continuity of Operations Plan (COOP).
    5. Collaboration - Anytime, Anywhere, Any Device: Leverage Corporate Knowledge and Capabilities.
    6. On-boarding/Usability- How to Make Best Use of Technology Offered.
    7. Authentication - Anywhere, Any Device: Single Sign-on.

h. Modernize the GSA network infrastructure by transitioning to a carrier managed, full mesh Multi-Protocol Label Switching (MPLS) network. GSA seeks to migrate to carrier managed routers for its core backbone, regional office buildings and select field office locations. GSA anticipates transitioning from Networx to a new contract vehicle in 2017.

i. Enable capacity and performance management via automated dashboards - providing GSA IT decision makers the real-time situational awareness to enhance the GSA Enterprise user experience.

C.5 TASKS

C.5.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT SUPPORT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the task/subtasks identified in this PWS.

The contractor shall designate a Program Manager (PM) by name for all programmatic issues/concerns/status. The PM shall be responsible for overall execution of this TO and shall have full authority to make decisions and commit the contractor's organization under this TO. The PM shall be readily available to respond to GSA's questions, concerns, and comments, and shall be proactive in alerting GSA to potential contractual issues including situations that may compromise the contractor's ability to provide the required services.

The contractor shall schedule meetings and provide deliverables in accordance with Section F.

C.5.1.1 SUBTASK 1 – COORDINATE A PROGRAM KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Program Kick-Off Meeting at a location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include vital contractor personnel, GSA IT Technical Point of Contact (TPOC), representatives from the GSA IT directorates, the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer (CO) and Contracting Officer's Representative (COR), and other relevant Government personnel. The contractor shall provide the following at the Program Kick-Off Meeting in accordance with Section F:

a. Draft Transition-In Plan
b. Program Management Plan (PMP) and all its sub-plans as described in Section C.5.1.5.

C.5.1.2 SUBTASK 2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (sample template shown in Section J, Attachment B) using Microsoft (MS) Office Suite applications and/or Google Applications, by the 10th of each month (EVM and financials, paragraphs g, h, and i below due by the 15th of each month) via electronic mail to the TPOC and the COR. The MSR shall include at a minimum the following:

a. Activities during reporting period, by task and subtask (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.

c. Personnel gains, losses, and status (to include GSA Homeland Security Presidential Directive (HSPD)-12 badging status, security clearance, etc.).
d. Government actions required.
e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken, conferences attended, etc.
g. Earned Value Management (EVM) statistics for projects as stated in H.19.
h. Accumulated invoiced cost for each subtask through the previous month.
i. Spend Plan to include projected cost of each CLIN, task and subtask for the current month and out months for the yearly period of performance.

C.5.1.3 SUBTASK 3 - EARNED VALUE MANAGEMENT (EVM)

The contractor shall employ and report on earned value in the management of this TO. See H.19, Earned Value Management**,** for the EVM requirements. The contractor shall coordinate with the Government to determine which of the controls in the American National Standards Institute (ANSI) Standard are applied to innovations and enhancement projects in order to ensure an optimal solution. The contractor shall execute EVM program control for non-operational tasks where projects are estimated at $250,000 or more or as otherwise specified by the TPOC/COR. The COR/TPOC will provide in writing to the contractor where and when EVM is applicable in regards to this TO. EVM controls being applied may vary from project to project as applicable.

C.5.1.4 SUBTASK 4 – CONVENE TECHNICAL STATUS MEETINGS

The contractor shall convene monthly Technical Status Meetings with the TPOC, COR, and other Government stakeholders. The purpose of these meetings is to ensure all stakeholders are informed of the monthly activities, review specific issues identified in the MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the TPOC and COR within two workdays following the meeting.

The contractor shall convene Weekly Operational Meetings with the TPOC, COR, and other Government stakeholders. The contractor shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the TPOC and COR within two workdays following the meeting. The purpose of these meetings is to:

a. Provide insight into operational status, issues, and concerns to cross-functional GSA IT managers.
b. Provide project status.
c. Review operations risk and security.
d. Provide system analytics (performance and capacity management).

C.5.1.5 SUBTASK 5 – PREPARE A PROGRAM MANAGEMENT PLAN (PMP) AND SUB-PLANS

The contractor shall document all support requirements in a PMP. The PMP shall:

a. Describe the contractor's management approach.
b. Include a list of all Standard Operating Procedures (SOPs) with version/date for all tasks/subtask.
c. Include a schedule of milestones, tasks, and subtasks required in this TO.
d. Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between or among Government organizations.
e. Include the contractor's EVM Plan.
f. Include the contractor's Concept Of Operations (CONOPS) Plan. The CONOPS shall include the organization chart, staffing plan to include staffing hours of availability versus on-call staffing, facility locations and contact information for the main POCs, timelines, general operating procedures, escalation procedures for after-hours support, staff training policies, transition plans, and any additional information the contractor considers relevant.
g. Include the contractor's Communications Plan.
h. Include the contractor's Risk Management Plan.
i. Include the contractor's Change Management Plan to address the requirements of Section C.5.4.2 and C.5.1.9.
j. Include the contractor's Quality Management Plan (QMP).

The contractor shall provide the Government with a draft PMP at the Project Kick-Off Meeting, on which the Government will make comments. The final PMP shall incorporate the Government's comments all according to Section F of this TO.

C.5.1.6 SUBTASK 6 – UPDATE THE PROGRAM MANAGEMENT PLAN (PMP) AND SUB-PLANS

The PMP is an evolutionary document that shall be updated twice yearly at a minimum. The contractor shall work from the latest Government-approved version of the PMP.

C.5.1.7 SUBTASK 7 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the Request for Travel is submitted. The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, dates and duration of trip, purpose of trip, and Point of Contact (POC) at travel location.

C.5.1.8 SUBTASK 8 – PROVIDE RECORDS MANAGEMENT

The contractor shall create and maintain files that document the processing of work products, deliverables and other associated information pertaining to tasks performed under this TO. The contractor shall provide a GEO portal where all files will be stored and maintained. Examples of files include the following:

a. Documentation providing traceability and rationale for the contractor's technical program decisions.

b. The latest internally controlled version of all specifications, drawings, databases, and software that define or implement the system.
c. Detailed Standard Operating Procedures
d. All configuration management documentation.
e. TO work products and deliverables.

The contractor shall provide GSA IT access to all records to ensure mission support is not interrupted. Upon completion of the TO, the contractor shall turn over all such records to GSA IT in approved formats according to Section F.5.3.

C.5.1.9 SUBTASK 9 – PROVIDE COMMUNICATIONS SUPPORT SERVICES

The contractor shall provide the following communication support services to maximize IT efficiency and stakeholder satisfaction throughout the GSA enterprise:

a. *Strategic Communications*: proactively deliver an ongoing campaign to identify IT tasks which can be solved by the end user without help desk support; draft communication (e.g., web pages, emails) to guide users through the self-help steps; and promote that content.
b. *Operational Communication*: develop and deliver communications about GSA IT systems and tools. Communications shall use all channels, including using emails, posters, social media, and GovDelivery. Communications shall be both broadcast (all GSA employees) and targeted (for example, all users of a certain device or all users in a certain region). Subject matter shall include system outages, system updates, and other end-user-targeted information.
c. *Data Analytics*: provide frequent reviews of data such as help desk tickets, web analytics, surveys, and social media interactions to determine audience needs and deliver information to end users to achieve strategic goal of expanding end-user knowledge and self-help processes of IT systems. This review shall include a report and recommendations for content management. Assist with implementing those recommendations and tracking their impact.
d. *Change Management*: develop campaigns of both communication and training to facilitate maximum user adoption with new and existing systems. This shall require working in concert with IT project teams and GSA's Office of Communications and Marketing.
e. *Usability and Accessibility*: identify and implement ways to make all end-user-targeted content compliant with Section 508 of the Americans with Disabilities Act, as well as using best practices for User Experience.

C.5.1.10 SUBTASK 10 – PROVIDE GENERAL LITIGATION IT SUPPORT SERVICES

The contractor shall support investigations related to Litigation Holds and Office of Inspector General. A Government point-of-contact will coordinate and manage requests for these services and will set the parameters of the information required, including the identified user account name(s) and time period(s). Under this subtask, the contractor shall:

a. Respond to subpoenas, discovery requests, court orders, and other matters related to litigation or Inspector General Inquiries that require the discovery, production, archiving, retention, or rotation of end user electronic information and Internet/Intranet activity information. Such assistance shall not include any subjective decision making by contractor.
b. Recover network backup-tapes for up to 30 calendar days from the date requested, including where, how, and when the electronic information on the backup tapes was collected and recovered.
c. Preserve relevant network backup information, including taking network media out of the contractor‘s network backup rotation and storing as required to respond to Government litigation needs until the litigation hold has ended.
d. Discontinue routine destruction of impacted records during litigation hold.
e. Locate, secure, and preserve, within reason, those records found in contractor-controlled on-line and off-line storage. A single litigation hold notice may cover one, few, or many different categories of records. In addition, the contractor shall search user-controlled, on-line storage areas of specified users.
f. Collect data from desktops, laptops, or mobile devices, including sector-by-sector imaging that preserves the integrity of the original data and metadata.
g. Perform periodic audit planning for electronic records, including conducting audits as directed by the Government and providing reports of compliance on a periodic basis.
h. Maintain a record of actions on each litigation hold request and report the status of litigation holds to the Government upon request. Upon request, the contractor shall report, for each litigation hold request, a description of the records preserved, including their quantity, category, file type, and location.
i. Utilize any means generally accepted in the industry for preserving evidence in anticipation of litigation if the Government does not specify the manner or method of performance for the litigation hold (A generally accepted preservation method would be to make a read-only copy of the pertinent native files on a hard drive or portable media with back-up copies stored at a different site).
j. Produce all responsive records found as soon as practical and give to the Government as soon as practical.

C.5.1.11 SUBTASK 11 – EXECUTE TRANSITION-IN

The contractor shall execute the Government-approved Transition-In Plan detailing the risks, milestones, dependencies, complexities, and hurdles and the corresponding solution set of processes, methodologies, and strategy to phase-in the proposed solution and seamlessly transition from the incumbent contractor. The draft Transition-In Plan provided with the contractor’s proposal shall be updated and delivered at the Program Kick-Off Meeting in accordance with Section F.

The contractor shall ensure that there will be no service disruption to vital Government business and no service degradation during and after transition.

GSA anticipates a transition period lasting between 90-120 days. The contractor shall perform all services, tasks, and any other support activities required to transition service operations from the

outgoing contractor during this period culminating with the cutover to be negotiated by the Government. The contractor shall propose a solution to seamlessly transition work from the incumbent contractor and baseline the services as currently provided.

Once services are fully transitioned and stabilized and the outgoing contractor transition-out period has ended, the contractor, with Government approval shall begin transformation from the inherited as-is environment to the contractor's proposed solution.

C.5.1.12 SUBTASK 12 – PREPARE AND EXECUTE A TRANSITION-OUT PLAN

The contractor shall prepare and deliver to the Government a Transition-Out Plan that facilitates the accomplishment of a low risk transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The Transition-Out Plan shall be delivered according to Section F.

When requested by the Government, in the event that responsibility for fulfillment of the GSA tasks described in this PWS, either in whole or in part, are transferred to a new contractor or the Government, the contractor shall participate in transition-out meetings with the PM, project staff, and representatives of the successor contractor and /or Government personnel. The purpose of these meetings will be to review project materials and take preparatory steps to ensure an effective transition in contractor support. When requested, the contractor shall develop, document, and monitor the execution of a Transition-Out Plan that may be used to transition tasks and materials described in this PWS to a new contractor or to the Government.

At minimum, the plan shall include the following:

a. Inventory of all services and materials required to fully perform the TO requirements.
b. Schedule of briefings, including dates, times, and resources allotted, that will be required to fully transition all materials developed to the follow-on contractor.
c. Names of individuals who will be responsible for fully briefing their follow-on counterparts.
d. Project management process.
e. Location of technical and project management documentation to include any standard operating procedures developed under this TO.
f. Appropriate contractor–to-contractor coordination to ensure a seamless transition.
g. Transition of Key and non-Key Personnel.
h. Schedules and milestones.
i. Actions required of the Government.
j. Knowledge transfer and training on key tools, policies, procedures and automation in the GSA IT environment.
k. A flexible and adaptive approach to accommodate the incoming contractor.
l. Data and system transfer methodology and schedule (e.g. Enterprise IT Services Dashboard).

The contractor shall implement its Government-approved Transition-Out Plan no later than (NLT) 90 calendar days prior to expiration of the TO as detailed in Section F of this TO.

C.5.1.13 SUBTASK 13 –CONTINUOUS SERVICE IMPROVEMENT (CSI)

The contractor shall provide continuous improvement services to enable GSA IT to reach new levels of performance while reducing costs. In partnership with GSA IT, the contractor shall recommend processes and technology improvements (tools, processes, methodologies, etc.) that will increase efficiency and enable GSA IT to continue to provide best value services to its customers. The contractor shall identify improvements and establish a baseline as a benchmark for metrics. After approval by the TPOC or designee, the contractor shall implement support recommendations and track the progress by capturing metrics against projected improvement. The contractor shall establish and maintain a CSI register. The contractor shall report on performance of implemented support improvements, issue reports on IT service area performance, and identify possible product/service enhancement opportunities for improved performance and potential cost savings.

The contractor shall develop and maintain an effective Quality Management System (QMS) that provides a standard, formal, and consistently applied approach for quality management, including quality requirements and criteria, key IT processes and their sequence and interaction, and the policies, criteria and methods for defining, detecting, correcting and preventing non-conformity and potential quality gaps. The contractor shall:

a. Develop and maintain a QMP for this TO that documents the structure, responsibilities, and procedures required to achieve effective quality management through planned and systematic activities, including industry standards such as ITIL, Federal Information Security Management Act (FISMA) and business requirements established by GSA operating units;
b. Document the standards, guidelines, and processes to monitor, measure, adjust and report quality indicators of performance;
c. Verify project products and activities against the applicable procedures and standards documented in the QMP;
d. Include a Customer Satisfaction Program (CSP) in the contractor's QMP. The CSP shall include monthly, quarterly, and annual customer assessments and reviews and shall be reported in the Monthly Status Reports;
e. Make the QMP and CSP available for government review and approval;
f. Establish, maintain, and update a QMS documentation repository where all quality management records, reports, and plans are stored and provide Government free and open access to the repository at all times.
g. Implement an outreach program to include town hall meetings and other stakeholder sensing methods to define possible areas of improvement.

C.5.2 TASK 2 - PROVIDE IT SERVICE STRATEGY SUPPORT

The contractor shall provide GSA with overarching IT Service Management strategic guidance and planning for obtaining and providing innovative and optimal service and performance delivery across the enterprise.

C.5.2.1 SUBTASK 1 - PROVIDE STRATEGIC PLANNING SERVICES

The contractor shall provide recommendations on the design, development, implementation, and maturation of IT service management, not only as an organizational capability, but also as a strategic asset. The contractor shall provide recommendations on the principles underpinning the practice of IT service management to aid the development and maturation of GSA IT service management policies, guidelines, and processes.

The contractor shall assist GSA IT in translating IT strategic goals, commitments and objectives into actionable plans, tasks, activities, technology and/or process solutions, possible alternatives, the estimated costs for the various options, and the potential risks associated with each alternative.

The contractor shall develop and implement IT Service Management Plans, practices, infrastructures, and systems utilizing industry best practices to optimize enterprise-wide IT service delivery and improve operational performance with minimal impact on the IT enterprise.

C.5.2.2 SUBTASK 2 - PROVIDE SERVICE FINANCIAL MANAGEMENT

The contractor shall provide financial information and management for IT services delivered under this TO. The contractor shall identify charges to internal and external clients according to use (i.e. a functioning equitable and transparent service charge back mechanism in place across the enterprise). The contractor shall identify IT services assets and customers, assist with the valuation of services and once approved report the costs by asset and customer. The contractor shall recommend and develop chargeback models for new and existing services.

C.5.2.3 SUBTASK 3 - PROVIDE SERVICE PORTFOLIO MANAGEMENT

The contractor shall assist GSA IT in managing an enterprise-level IT service portfolio that provides customers with a pre-defined set of available GSA IT products and services. The contractor shall identify, prioritize, and recommend service opportunities that create business value. The contractor shall manage the portfolio of services delivered under this TO. The contractor shall maintain a complete and accurate service pipeline list of all services under consideration or development; a service catalogue of all operational services and those available for deployment; and a repository containing information about services that are phased out or retired.

C.5.2.4 - SUBTASK 4 - PROVIDE SERVICE DEMAND MANAGEMENT

The contractor shall perform activity-based demand management. The contractor shall assist GSA IT with the analysis of business activity and user profiles that generate demand, and develop forecasts for expected changes in service demand and future IT resource capacity and availability requirements. The contractor shall recommend and develop business cases for new technologies to meet demand. The contractor shall recommend techniques to influence and manage demand in such a way that excess capacity is reduced but the business and customer requirements are still satisfied.

In response to capacity, workforce, or workspace changes, the contractor shall complete the following:

a. Conduct a trend analysis on historical data to assess future user IT provisioning needs.

b. Review license usage and availability to potentially reduce costs to GSA.
c. Perform capacity planning for workforce changes.
d. Review maintenance agreements to identify, address, and plan for pending termination dates.
e. Analyze changing needs across organizations and sites to make recommendations for allocation or reallocation of existing IT resources.
f. Summarize recommendations in the Service Improvement Plan as described in Section C.5.3.6.

The contractor shall provide Demand Management Reports as stated in Section F.

C.5.2.5 SUBTASK 5 - PROVIDE COMPLIANCE MANAGEMENT

The contractor shall provide a well-defined review and reporting process that shall ensure compliance with all applicable laws, regulations, mandates, executive orders, directives, and contractual requirements stipulated by GSA and any other applicable compliance requirements stipulated by an issuing Governmental body. The contractor shall monitor and report proposed or pending new governmental, legal, regulatory, and contractual compliance requirements that will require any modification, alteration, or change in service delivery. The contractor shall analyze new or changed compliance requirements for impact and recommend appropriate alternative courses of action to facilitate compliance. The contractor shall identify, develop, and document detailed plans for implementing approved changes in service management and delivery.

C.5.3 TASK 3 - PROVIDE SERVICE DESIGN SUPPORT

The contractor shall provide GSA IT service design support to include infrastructure, communication, and material components in order to improve quality of the service and the productive interaction between service and end user. The contractor shall develop service design methodologies that align front and back office services to the needs of the end user so that the service is user-friendly, relevant, and sustainable. The scope of service design is not limited to new services. It includes the changes and improvements necessary to increase or maintain value to customers over the lifecycle of services, the continuity of services, achievement of service levels, and conformance to standards and regulations.

C.5.3.1 SUBTASK 1 - PROVIDE EMERGING TECHNOLOGY AND INNOVATION SERVICES

GSA IT requires continual improvement within its enterprise to drive efficiencies while offering enhanced support to its diverse and mobile client base. GSA IT has been tasked with achieving continual cost reductions in service through innovation, automation, and process refinement. GSA IT requires a methodology to enable piloting and testing to ensure that recommended technologies or enhancements do not disrupt or degrade operational services to GSA IT customers.

As part of the Emerging Technologies and Innovation Services, the contractor shall:

a. Establish an engineering function and innovation process to infuse innovation into program solutions and operations when approved by the Government. The engineering function shall support the full range of infrastructure engineering design, enterprise

architecture standards, prototyping, integration, including, but not limited to, concept development, planning, requirements definition and analysis, systems design, integration, and deployment.

b. Maintain a lab environment for testing and piloting new and enhanced technologies.
c. Develop and implement service design principles, practices, and methodologies to convert GSA IT strategic objectives into actionable and supportable portfolios of well integrated IT services and service assets.
d. Develop and maintain a holistic forward-looking IT Optimization and Transformation Plan to incrementally transform GSA IT services and infrastructure, where emerging technologies provide a more resilient and agile business environment. The IT Optimization and Transformation Plan shall take into consideration:
    1. Technical solutions for a GSA Network that can transform from supporting single-vendor, private data center service and privately-owned Wide Area Network (WAN) to a multi-vendor, hybrid private-cloud and public-cloud service, and managed network.
    2. Benefits offered by a Software-Defined Networking (SDN)-based network at WAN, Local Area Network (LAN), and Data Center level
e. Innovate (create new) or improve (modify existing) services to make them more useful, usable, desirable for customers, and efficient as well as effective for the organization.
f. Research and evaluate new and emerging technologies within all areas of GSA IT service delivery for integration into the GSA IT operational environment upon request of the Government.
g. Develop an Emerging Technology and innovation Plan and report findings and make recommendations with emphasis on how the new technologies innovation will enhance service or improve customer use while driving efficiencies in terms of cost or performance.
h. Document the engineering design of any recommended prototype so that it can be used to facilitate a pilot phase or detailed service design plan.
i. Propose methodologies to utilize open networking protocols and/or open sources within GSA IT infrastructure while minimizing service degradation.
j. Develop and perform pilot programs to ensure recommended technologies or enhancements do not disrupt or degrade operational services to GSA IT customers.
k. Provide strategy and design support for other Information Technology Service Management (ITSM) areas such as Service Operations.

C.5.3.2 SUBTASK 2 - PROVIDE INFRASTRUCTURE ARCHITECTURE SERVICES

GSA IT requires infrastructure architecture support services to align GSA Enterprise capabilities to the vision and direction of the overall GSA Enterprise Architecture (EA) effort. This will ensure the GSA Enterprise IT Service delivery can effectively support the current and future IT requirements of the GSA business portfolios. GSA's EA program spans six sub-architectural domains: strategy, business, data, applications, infrastructure, and security. GSA IT is looking to the contractor to assist in providing and maintaining the infrastructure sub-domain's metadata.

The contractor shall provide the following infrastructure architecture services:

a. Coordinate and work with GSA IT and its EA program office to determine business process and productivity needs and an appropriate technology strategy to support business goals as it affects the Infrastructure Architecture Domain. The contractor shall analyze technical needs, requirements, and state of the network's infrastructure design, integration, and operations. The contractor shall recommend and implement approved cost-cutting technologies and methods to increase efficiency and reduce the overall cost of GSA IT's operations and infrastructure for the business.
b. Coordinate and work with GSA IT management and its EA program office to architect and document the as-is and to-be IT infrastructure and networks that effectively reflect business needs, service-level and availability requirements, and other technology parameters.
c. Develop, propose, and maintain design principles, models, plans, internal standards, and processes as defined by the Technical Standards Profile and other metadata attributes in GSA IT's EA repository (currently in IBM System Architect) in accordance with the Common Approach to Federal Enterprise Architecture (CAFEA) (May 2, 2012) or revised guidance as updated by GSA IT's Enterprise and Planning Division. (For additional reference see also: ITIL 2011 edition, TIA-942-2 Data Center Standard (March 2010) and Building Industry Consulting Service International Incorporated (BICSI) 002-2010 Data Center Design and Implementation Best Practices.)
d. Recommend IT technologies and products for implementation; leading teams of other infrastructure technicians and engineers in developing detailed designs and quality control mechanisms during implementation.
e. Actively maintaining GSA IT's System Architect (SA) metadata concerning the Infrastructure Architecture Domain defined below in accordance with the CAFEA:
    1. High-Level Network Diagram (I-1)
        i. Describes the means by which data flows between systems.
    2. Hosting Concept of Operations (I-2)
        i. Presents the high level functional architecture, organization, roles, responsibilities, processes, metrics, and strategic plan for hosting and use of hosting services.
    3. Technical Standards Profile (I-3)
        i. Defines the various systems standards that implement and sometimes constrain the choices that can be made in the design and implementation of an architecture.
    4. Technology Forecast (I-4)
        i. The emerging technologies, software/hardware products, and skills that are expected to be required in a given set of time frames and that will affect the future infrastructure.
    5. Cable Plant Diagram (I-5)
        i. Diagrams the wires and connectors used to tie a network together.
    6. Wireless Connectivity Diagram (I-6)

i. Diagrams a communications network that provides connectivity to wireless devices.

7. Rack Elevation Diagrams (front and back) per GSA Telecommunication Distribution Design Guide (TDDG) (I-7)
    i. Two-dimensional elevations, drawn to scale and showing everything that needs to be placed in a certain area, that describe the organization of specific equipment on a rack.
8. Data Center/Server Room Diagram (I-8)
    i. Diagrams the layout and contents of a data center or server room.
9. Wiring Closet Diagram (I-9)
    i. Diagrams the layout and contents of a wiring closet.
10. Point of Presence Diagram (I-10)
11. Asset Inventory (I-11)
    i. A list of assets with details about each (installation date, location, original cost, condition (e.g., in-service, in inventory, excessed), and such.

C.5.3.3 SUBTASK 3 - PROVIDE CAPACITY MANAGEMENT SUPPORT

The contractor shall provide capacity management services to ensure the capacity and performance of the GSA IT infrastructure meets the demand profile of GSA's evolving business environment in the most cost-effective and timely manner. The contractor shall perform the following key capacity management activities:

a. Develop, document, and maintain capacity management processes and procedures that meet requirements.
b. Implement agreed-upon capacity management processes and procedures.
c. Establish a comprehensive capacity management planning process.
d. Develop and maintain Capacity Plans which will meet demand and SLRs.
e. Define, develop, and implement tools that allow for the effective capacity monitoring/trending of IT infrastructure, applications, and IT components.
f. Continually monitor IT resource usage to enable proactive identification of capacity and performance issues.
g. Assess incidents/problems related to throughput performance.
h. Perform tuning activities to improve IT infrastructure capacity and performance (under the control of change management).
i. Capture trending information and forecast future GSA IT capacity requirements based on GSA IT defined thresholds.
j. Recommend changes to capacity to improve service performance.
k. Maintain capacity levels to optimize use of existing IT resources and minimize GSA IT costs to deliver services at agreed-to SLRs.
l. Identify financial impacts of capacity plans.
m. Conduct risk assessment of capacity recommendations.

n. Provide the following deliverables in accordance with Section F:

1. Capacity Management Plan: The Capacity Management Plan details current performance and utilization, future requirements, capacity projections, capacity issues, and plans for improving performance and satisfying business requirements. The Capacity Management Plan will also include the Capacity Management Processes and Procedures.
2. Capacity Management Reports to include:
    i. Service Performance Information and Reports: Reports on the performance and utilization of services using data in the CMIS.
    ii. Component Performance Information and Reports: Reports on the performance of Components using data in the CMIS.
    iii. Workload Analysis and Reports: Reports providing information about workloads that can be used for modeling, application sizing, and capacity planning.
    iv. Ad Hoc Capacity and Performance Reports: Performance and utilization reports generated on an as needed basis, typically in response to capacity issues.
    v. Forecasts and Predictive Reports: Reports used to plan capacity changes and proactively identify potential capacity issues.

C.5.3.4 SUBTASK 4 - PROVIDE AVAILABILITY MANAGEMENT SUPPORT

The contractor shall perform availability management services to ensure the capability of GSA IT infrastructure and services are optimized to deliver a cost-effective and sustained level of service availability to meet GSA's evolving business requirements. Availability management includes the evaluation, design, implementation, measurement, and management of the infrastructure availability from a component and an end-to-end perspective, including new or modified IT service management methodologies and tools, as well as technology modifications or upgrades of IT infrastructure systems and components. The contractor shall provide the following key availability management activities:

a. Draft availability management policies and procedures and recommend appropriate availability management tools and methods that support GSA IT availability management support requirements.
b. Implement agreed-upon availability management policies and procedures and supporting processes.
c. Perform regular reviews of the availability management processes, procedures, and associated techniques and methods to ensure that all are subjected to continuous improvement and remain fit for purpose.
d. Produce and maintain a forward-looking Availability Management Plan that prioritizes and plans overall availability improvement.
e. Ensure that availability requirements are included in new or enhanced service plans.

f. Identify business unit availability requirements for new or enhanced services and formulate the availability and recovery design criteria for the infrastructure to ensure services are designed to deliver the appropriate levels of availability.
g. Identify the critical business functions and impact arising from IT component failure. Where appropriate, review the availability design criteria to provide additional resilience to prevent or minimize impact to the business.
h. Identify opportunities to optimize the availability of the infrastructure to deliver cost-effective improvements that deliver tangible business benefits.
i. Conduct availability assessment review sessions and provide cost-justified improvement recommendations.
j. Ensure that all availability management improvement initiatives conform to defined change management procedures.
k. Monitor and trend analysis of the availability, reliability, and maintainability of systems and components.
l. Review service, system, and component availability, identify unacceptable levels, and ensure appropriate corrective actions are taken to address availability shortfalls.
m. Investigate the root cause for unacceptable levels of availability.
n. Participate in problem management review sessions as appropriate, specifically those problems related to outages of critical systems.
o. Coordinate with the GSA IT and third-party vendors to research, review, and assess availability issues and optimization opportunities.
p. Assess the impact arising from IT service and component failure in conjunction with Service Continuity Management and, where appropriate, review the availability design criteria to provide additional resilience to prevent or minimize impact to the business. Implement cost-justifiable countermeasures, including risk reduction and recovery mechanisms.
q. Coordinate with GSA IT and third-party service providers to gather information on IT systems and service availability issues and trends to be used for trend analysis.
r. Provide a range of availability reporting to ensure that agreed-upon levels of availability, reliability, and maintainability are measured and monitored on an ongoing basis.
s. Participate in user requirements gathering and analysis when new IT systems and services are being defined to ensure that IT services and systems are designed to deliver the required levels of availability required by the business.
t. Participate and cooperate with GSA IT in defining availability Service Level Requirement (SLR) measures and reporting requirements.
u. Recommend appropriate tools and practices to measure and report on agreed-upon availability SLRs for new and enhanced IT Infrastructure.
v. Implement agreed-upon availability SLR measurement tools and practices.
w. Monitor actual IT availability achieved versus targets and ensure shortfalls are addressed promptly and effectively.

x. Monitor and maintain an awareness of technology advancements and IT best practices related to availability optimization and periodically provide updates to GSA IT management.
y. Provide the following deliverables in accordance with Section F:
    1. Availability Management Plan to include :
        i. Availability Management Processes and Procedures
        ii. Measures of availability and agreed on availability targets
        iii. Availability Improvement Plans
        iv. System Recovery Strategies
    2. Availability Management Reports:
        i. Monitoring and Reporting of Availability, Reliability, and Maintainability
        ii. Unavailability Analysis Reports
        iii. Forecasting Reports

C.5.3.5 SUBTASK 5 - PROVIDE INFORMATION SECURITY MANAGEMENT SERVICES

The contractor shall provide system security support to maintain and enhance the security fabric of GSA's infrastructure by monitoring and managing security risks in cooperation with GSA IT Security staff assigned to Information Security (IS). This includes coordination of regular updates of the Enterprise IT Infrastructure Security Plan as an overarching plan with an objective of ensuring that all appropriate GSA and Application System's plans, when examined together, provide the appropriate level of coverage of security appropriate to the overall GSA IT infrastructure and Government requirements. The contractor shall provide the following security and FISMA services:

a. Support the development, creation, and revision of any Interconnection Security Agreements and supporting Memorandum of Agreement/Understanding (MOA/U), completed in accordance with National Institute of Standard and Technology (NIST) 800-47, "Security Guide for Connecting Information Technology Systems," for existing and new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, Virtual Private Network (VPN), etc. Interconnections agreements shall be submitted as appendices to the System Security Plan for appropriate FISMA systems.
b. Provide updated status to assigned Information System Security Officer concerning the Plan of Action and Milestones (POA&M) of respective FISMA systems for mitigation and improvements on a quarterly basis.
c. Conduct security-related tasks using automated methods whenever possible, to minimize security risks, alert GSA to potential issues, and allow for regular scrutiny of operations for any abnormalities in coordination with IS staff, ISSOs and Information System Security Managers as requested.
d. Provide server security services oversight and guidance related to hardening and Windows Group Policy Object (GPO) administration, basic intrusion detection, antivirus,

and access control. The contractor shall also provide notification of security breaches and implement corrective actions to rectify risks and secure resources and information and perform ongoing security diligence and recommendations to improve security monitoring to appropriate Government officials and offices.

e. Coordinate and assist GSA IT in the necessary activities and in providing the necessary documentation to meet FISMA security requirements and GSA Policies for a Moderate Impact" system. This requirement includes support for the following activities:
    1. Authorization and Accreditation Support
    2. Risk Management Register Development, Management, and Maintenance
    3. System Remediation Support
    4. System Hardening Support
    5. System Scanning Support
    6. Policy Modification Support
    7. Process/Procedure Development Support
f. Identify security monitoring improvement opportunities for all GSA enterprise IT infrastructure systems.
g. Coordinate and assist GSA IT to ensure all systems are protected against external and internal security threats.
h. Coordinate and assist GSA IT to ensure all systems have Authority to Operate (ATO).
i. Coordinate and assist GSA IT to ensure new systems have Interim ATO at the appropriate time.
j. Coordinate and assist GSA IT to maintain authentication venues for the enterprise and appropriate business line applications.
k. Coordinate and assist GSA IT to ensure security tasks comply with the latest version of all applicable regulations, policies, procedures, and standards.

C.5.3.6 SUBTASK 6 - SERVICE LEVEL MANAGEMENT

The contractor shall provide service level management to ensure GSA IT services are delivered to the agreed upon service and quality levels and that they match the expectations and business needs of the customer in a cost-effective manner. Service levels will change throughout the life of the TO as the posture of GSA IT changes.

The contractor shall manage, monitor, measure, and report on the ongoing overall service delivery performance across all IT service areas with the overall goal of improving them at an acceptable cost. Reports shall provide performance analysis and assessment of each individual IT service area, as well as incorporate an analysis and assessment of the overall end-to-end performance achievement obtained across all service areas.

The contractor shall report service level performance through the Enterprise IT Services Dashboard as specified in Subtask C.5.3.8. The contractor shall review the current set of performance tools in use by GSA IT and identify any gaps in capability to fulfill the requisite monitoring, measurement, management, analysis, and reporting requirements. The contractor

shall document and report its findings, which shall include potential alternative courses of action to resolve the gaps.

The draft SLAs contained in Attachment G provide a summary of high level minimum performance levels for service operations. GSA views this reference as representative of performance for the current environment (status quo). GSA is seeking to improve the service it provides to customers through more innovative methods or approaches that align with ITSM best practices and is interested in measures more accurately tied to the contractor's specific technical approach and that, when met or exceeded, provide unified, continuous, end-to-end service delivery that results in high customer satisfaction. The expectation is that the measurements and monitoring (possibly addressing more than one area of service in a single metric) will result in a more holistic approach and view of system performance.

The contractor shall develop and deliver Operational Level Agreements (OLA) within 60 calendar days of Project Start. OLAs will address all services provided by the contractor that require activities by GSA IT staff and GSA contractors to support delivery of services under this PWS. The Government will provide feedback for incorporation into OLAs. OLAs shall be reviewed and updated quarterly to allow for incorporation of new services as they are deployed.

The contractor shall provide the following deliverables in accordance with Section F:

a. Service Quality Plan (SQP) - The contractor shall deliver a SQP which defines a formal methodology by which to assess the quality of services being provided and specifies the quality standards, practices, resources, specifications, and the sequence of activities of a standards-based Quality Control (QC) approach as a part of Service Level Management. This plan will supplement the QMP's structure, responsibilities, and procedures and will include the processes to monitor, measure, adjust and report on quality indicators of performance as specified in subtask C.5.1.13.
b. Service Level Requirements (SLRs) - The contractor shall assist in developing SLRs that focus on GSA IT customers and their business needs for new and existing services. The contractor shall document SLRs that include detailed information about the customer's needs and expectations in terms of performance and level of service.
c. Service Level Agreements (SLAs) - The contractor shall assist in defining key IT service performance indicators that clearly define the essential aspects of the service (such as description, availability, quality levels, recovery times, etc.) in a Service Level Agreement (SLA).
d. Service Improvement Plans (SIPs) - The contractor shall review, evaluate, and prepare reports on the quality of service and SIP when service delivery does not meet SLRs or when greater cost effectiveness is achievable. The SIP shall include clear milestones, which will enable GSA IT to determine whether or not timely progress is being made.
e. Service Level Management Plan (SLMP) - The contractor shall deliver a SLMP which provides the framework and outlines the processes involved in executing Service Level Management (SLM). The SLMP will provide high level lifecycle view and identify the key SLM tasks related to managing service level requirements, agreements, and improvements to ensure GEO services are delivered to the agreed upon service and quality levels. The SLMP shall describe the cradle-to-grave lifecycle of a service level and the processes for initiating service level requirements, agreements, and

improvements. The SLMP shall provide the methods, processes and frequencies for monitoring, measuring, and reporting service level performance and quality.

C.5.3.7 SUBTASK 7 - ENTERPRISE IT SERVICE MANAGEMENT

GSA's Enterprise IT Management (EITM) system provides management control across the enterprise through integration and automation of the management of IT applications, databases, networks, security, storage, and systems utilized by all departments and disciplines. This integrated solution directly supports GSA's business services and simplifies GSA IT's management and provisioning of unified IT services across the enterprise, resulting in enhanced business performance while providing comprehensive visibility into the quality, costs, and risks associated with the services provided.

The contractor shall leverage GSA's EITM system to the maximum extent practicable as the primary ITSM tool and in the management and delivery of IT services.

The contractor shall maintain a complete and accurate Service Catalogue of all operational IT services and those being prepared for production deployment.

GSA's EITM system consists of the following IT resource management solutions which will be provided for contractor use as Government-Furnished Property (GFP):

a. ServiceNow's Cloud Based Enterprise Edition Service Management Suite:
    1. ServiceNow Asset Management
    2. ServiceNow Change and Release Management
    3. ServiceNow Configuration Management
    4. ServiceNow incident Management
    5. ServiceNow IT Cost Management
    6. ServiceNow Problem Management
    7. ServiceNow Service Catalog
b. Cisco Unified Call Manager
c. Avaya System Management
d. Computer Associates IT Client Manager
e. Solar Winds
f. NetIQ Directory and Resource Administrator

The contractor may recommend additional EITM modules, APIs and licenses throughout the life of the TO to enhance performance and/or reduce operational costs.

The contractor shall provide operational and maintenance support for GSA's EITM system to include:

a. Operate and maintain the EITM system including software upgrades, system troubleshooting, and fulfilling access and applicable change requests.
b. Provide ServiceNow system administration, configuration, form tailoring, business process automation, and third-party integration and data import to support the

development, test, and production environments. This is inclusive of ensuring previously developed customizations stay current with GSA's organizational and workflow changes.

c. Manage and maintain dashboards that integrate information from all components of GSA's EITM system.
d. Maintain ITSM processes and workflows.
e. Manage the content and operations of GSA's Configuration Management Database (CMDB) including maintaining the logical service configurations of the infrastructure and applications supporting GSA's IT Services.
f. Complete lifecycle asset and configuration management including mapping the physical configuration and inventory data to the CMDB.
g. Maintain a comprehensive Service Catalogue of all operational IT services and those being prepared for production deployment.

C.5.3.8 SUBTASK 8 - ENTERPRISE IT SERVICES DASHBOARD

The contractor shall provide Enterprise IT Services Dashboard services. The Enterprise IT Services Dashboard shall provide automated and GSA IT accessible enterprise-wide metrics, statistics, and real-time data on Critical Success Factors and Key Performance Indicators (KPIs) regarding the provisioning of IT services to support performance management objectives and decisions regarding the investment and management of IT resources.

The contractor shall develop, implement, and maintain, in a readily accessible and easy-to-use format, the capability to display (report) information critical to GSA IT and GSA's customer base on an enterprise-wide basis including, but not limited to, system outages, applications issues, call-center statistics, critical IT services health and performance, and Service Desk Ticket status.

The Enterprise IT Services Dashboard shall have a web-based interface and shall use open source development to the maximum extent practicable. The Enterprise IT Services Dashboard shall not have any corporate markings referencing the contractor.

The Government shall own the Enterprise IT Services Dashboard system and data and both shall be transitioned as detailed in Section C.5.1.12.

C.5.3.9 SUBTASK 9 - IT SERVICE CONTINUITY MANAGEMENT

The primary objective of this task is to improve and maintain GSA's IT readiness response to planned and unplanned contingencies through exercise support and a viable COOP and Disaster Recovery (DR) Program for critical infrastructure and network security operations. National Security Presidential Directive-51 (May 9, 2007) (NSPD-51)/ HSPD-20 (May 9, 2007), National Continuity Policy specifies certain requirements for continuity plan development, including the requirement that all Federal executive branch departments and agencies develop an integrated, overlapping continuity capability. The range of recovery services under this functional area covers the spectrum from partial loss of function or data for a brief amount of time to a "worst-case" scenario in which a man-made, natural disaster, or IT failure results in the loss of the entire IT enterprise. Services may be required during any timeframe from initial declaration of a disaster to final recovery of all business processes. Cloud services should be leveraged to the maximum extent possible. The contractor shall provide a COOP Plan (IT Business Continuity

Plan), an IT Service Continuity Plan, Information System Contingency Plans (ISCPs) and services related to any and all methodologies pertaining to DR and business continuity to include:

a. Adhere to Agency COOP Plans and Mission Essential Playbooks.
b. Ensure standard and emergency processes and procedures are documented and submitted to the designated GSA authority and the GSA CO for approval before implementation.
c. Assist GSA in preparations necessary for recovery to an operational status and provide restoration services after each security event or incident as applicable.
d. Provide communications capability that permits management to coordinate recovery tasks across each of GSA's critical departments and the supporting functions for each of those departments.
e. Maintain a high level of readiness and be capable of implementation, both with and without warning.
f. Ensure that all support staff functions are designed such that no critical function poses a single point of failure.
g. Ensure timely and orderly recovery from an emergency and resumption of full service to reduce any complexity, confusion, or exposure to error that may occur.
h. Ensure the continuous performance of the agency’s essential functions/operations during an emergency.
i. Be operational no later than 12 hours after activation. Take maximum advantage of existing agency field infrastructures.
j. Maintain sustained operations for up to 30 days.
k. Participate in response team deployments for on-site support requirements on an as-needed basis.
l. Research, evaluate, and propose IT infrastructure at the COOP sites(s) on an ongoing basis.
m. Engineer data redundancy systems to ensure that critical files are available (as defined by the COOP Plan).
n. Assist the Government in designing and coordinating installation of necessary site telecommunications that provide multiple, highly redundant communications links as defined by the COOP Plan requirement.
o. Ensure that all availability, resiliency, and recovery mechanisms are appropriately tested on a regular basis to ensure optimum ongoing service and system delivery continuity and reliability.
p. Execute annual internal GSA testing and exercising of COOP plans and procedures to ensure the ability to perform essential functions and operate from designated alternate facilities.
q. Perform quarterly testing of alert and notification procedures and systems for any type of emergency.
r. Support tests, pre-incident training, and exercises in order to demonstrate and improve the agency’s ability to execute the plan.

s. Provide periodic training sessions and training aides to prepare GSA employees to use the specific technology and procedures during the COOP exercise.
t. Provide updated COOP plans and contingency plans as necessary and review and update the GSA IT playbooks in accordance with Section F.
u. Provide reconstitution, planning and testing methodologies.

In situations where impending or predictable events are anticipated (such as weather emergencies or transit strikes) GSA may direct and the contractor shall place employees in temporary quarters near GSA sites so that operations can continue. Allowable expenses for housing and meals will apply and will be reimbursed by GSA.

C.5.4 TASK 4 - PROVIDE SERVICE TRANSITION SERVICES

The contractor shall provide GSA with support for the full lifecycle of transition of service delivery technologies and end-user devices and equipment. The contractor shall plan and proactively manage resources to successfully add a new service to or change an existing IT service with minimal impact to the GSA IT infrastructure environment.

C.5.4.1 SUBTASK 1 - KNOWLEDGE MANAGEMENT SUPPORT

Knowledge Management includes the analysis, storage, sharing, and reuse of knowledge and information to improve efficiency by reducing the need to rediscover knowledge. The contractor shall perform knowledge management services to improve the quality of management decision-making by ensuring that reliable and secure information and data is available throughout the service lifecycle to include:

a. Assist GSA IT infrastructure operations with defining and developing clear cradle-to-grave knowledge lifecycle management processes and procedures.
b. Develop a practical approach to organizing and implementing knowledge management in a support environment that encompasses operational objectives in a knowledge initiative as well as providing tactical and managerial guidance.
c. Align processes to support knowledge creation and use that ensures effective integration and easy linkages between IT processes, especially between incident, problem, and knowledge management.
d. Automate the knowledge lifecycle to ensure quality and relevant content is produced in a timely manner.
e. Identify and create reusable content that is relevant and reflects real customer demand in the form of incidents and problems.
f. Simplify knowledge retrieval to allow customers to access knowledge content in context of the situation and process where and when they need it.
g. Measure knowledge creation and utilization, identify gaps and exceptions, and measure overall outcomes of knowledge management.
h. Maintain and enhance the Enterprise IT Service Desk knowledge base. Ensure resolved incidents are recorded in a corresponding Knowledge Base article.

C.5.4.2 SUBTASK 2 - PROVIDE CHANGE MANAGEMENT

The contractor shall provide change management services to include all activities to ensure that standardized methods and procedures are used for efficient and prompt handling of changes on an enterprise-wide and local/regional scale. The goal of change management is to manage the lifecycle of all changes in order to minimize the impact of change upon service quality and consequently to improve the day-to-day operations of the GSA IT infrastructure. Change Management covers all aspects of managing the introduction and implementation of changes affecting all services and in any of the management processes, tools, and methodologies designed and utilized to support service components. Change management processes are complementary to release management and configuration management, as well as incident management and problem management. The contractor shall work within the ITIL framework and follow GSA IT procedures for changes and incidents affecting any GSA IT system. The contractor shall perform the following key change management tasks under this subtask:

a. Identify the types of changes and establish appropriate change models, Change Authorization matrix and Change Advisory Board (CAB) membership.
b. Identify the change process owner, manager and develop a RACI matrix as they pertain to all types of changes.
c. Establish a change documentation and tracking system.
d. Conduct, maintain and support a Request for Change (RFC) process to include:
    1. Initial review, recording and filtering of change requests.
    2. Establishment of a Core-CAB and ancillary members.
    3. Assess/Evaluate required changes based on impact, risk, resources and make a recommendation to the appropriate change authority.
    4. Manage and Chair the weekly CAB meeting.
    5. Facilitate the change authorization process and maintain a change schedule and projected service outage register/report.
    6. Monitor the release and deployment process and report issues to the CAB and Change Authority.
    7. After Build/Testing is completed, ensure that formal authorization to deploy is granted and a remediation/back-out plan is in place before changes is released into production.
    8. Conduct a Post Implementation Review and closure of the change to include a verification that all testing, configuration, asset and service related information is updated.
e. Establish a Change Proposal method for major or high impacting changes.
f. Conduct a periodic review of all changes in order to identify areas for process improvement as well as determine if certain change frequencies justify the establishment of a standard change.
g. Participation in IT service continuity and DR planning.
h. Integrate with GSA IT change management policies, procedures, processes and training requirements per the change management process components outlined above, including

CCB composition, activities, and the financial, technical, and business approval authorities appropriate to GSA IT and business requirements.

i. Receive and document all RFC and classify proposed changes to the services, which shall include change cost, risk impact assessment, and system(s) security considerations.
j. Provide a change management plan to GSA IT for review.
k. Develop and maintain a schedule of planned approved changes (Forward Schedule of Changes (FSC)) and provide to GSA IT for review.
l. Provide change documentation as required, including proposed metrics as to how effectiveness of the change will be measured.
m. Participate in CCB meetings as GSA IT deems appropriate or necessary.
n. Monitor changes, perform change reviews and report results of changes, impacts, and change effectiveness metrics.
o. Verify that change met objectives based upon predetermined effectiveness metrics and determine follow-up actions to resolve situations where the change failed to meet objectives.
p. Define and support the Emergency CAB process and ensure that emergency changes are fully documented after release.

C.5.4.3 SUBTASK 3 - RELEASE AND DEPLOYMENT MANAGEMENT

The contractor shall schedule, implement and control approved changes to software and components that are required to support the infrastructure (e.g., virus detection software, software required to manage the Storage Area Network (SAN), backup software, retention of prior versions of production Operating Systems (OS), etc.), release, and deployment management activities and take a holistic view of a change to a service, including all aspects, technical and non-technical, software, hardware, and network changes. These changes can be implemented by rolling out a combination of new applications, infrastructure software, upgraded or new hardware, or simply by making changes to the service hours or support arrangements. Release and deployment management processes and activities are complementary to those of change management, configuration management, and problem management.

Releases typically consist of a number of problem fixes and enhancements to an existing service. A release consists of the new or changed software required and any new or changed hardware needed to implement the approved changes. Releases are generally divided into the following categories:

a. Major software releases and hardware upgrades or replacements, normally containing large areas of new functionality. A major upgrade or release usually supersedes all preceding minor upgrades, releases, and emergency fixes.
b. Minor software releases and hardware upgrades, normally containing small enhancements and fixes, some of which may have already been issued as emergency fixes. A minor upgrade or release usually supersedes all preceding emergency fixes.
c. Emergency software and hardware fixes, normally containing the corrections to a small number of known problems.

The contractor shall develop a Release and Deployment Management (RDM) Plan which will detail how the contractor will coordinate and deliver end-to-end release and deployment services in an ITIL-based framework.

The contractor shall provide the following key release and deployment management services:

a. Identify the RDM process owner and manager
b. Establish standardized release management policies and procedures.
c. Develop, manage, update, and maintain formal release plans and schedules for all planned releases.
d. Provide release management plans and schedules to GSA IT for review.
e. Establish and manage a release documentation and identification schema.
f. Validate that all releases have proper approval from change management prior to execution
g. Conduct and manage the release design, build, and configuration processes.
h. Rollout planning including quality plans and regression plans.
i. Provide release communication, preparation, and training.
j. Manage the successful rollout/distribution and installation of all elements of a release.
k. Ensure that only correct, authorized, and tested versions are installed and that changes are traceable and secure.
l. Establish and administer the version control schema as it relates to release management of GSA IT custom applications.
m. Develop quality plans and regression plans as appropriate for each release.
n. Ensure that any new software or support services required for the release are procured and available when needed.
o. Conduct and manage release testing and testing management.
p. Ensure that all necessary testing environments are available and properly configured to support release testing. Plan and manage the acceptance testing process for each release.
q. Ensure that thorough testing is performed prior to release and assess business risk related to any change that is not fully tested prior to implementation. (Submit a Test Plan for GSA IT approval prior to the start of test.)
r. Schedule and conduct release management meetings to include review of planned releases and results of changes made.
s. Identify and document all Configurable Items (CIs) that need to be included in the release, as well as all system interdependencies.
t. Provide release documentation as required and update all required knowledge management systems.
u. Provide early life support to Operations as required
v. Review release management details and alter as appropriate to meet the needs of the GSA IT (e.g., back-out plan, go/no go decision).
w. Notify GSA business unit affected applications “owners” of release timing and impact.

x. Implement release in compliance with change management requirements and adherence to detailed release plans.
y. Modify configuration database, asset management items, and service catalog (if applicable) to reflect changes to CIs due to the release.
z. Conduct post-mortem of releases that necessitated implementation of the regression plan and develop and implement appropriate corrective or follow-up actions to minimize future occurrences.

C.5.4.4 SUBTASK 4 - SERVICE VALIDATION AND TESTING

The contractor shall provide service validation and testing to include quality assurance and production control support services. The contractor shall automate validation and testing where feasible to gain efficiencies during the performance of the TO.

a. Service Validation and Testing (SVT) is planning and coordinating tests to ensure that specifications for the service design are met and validated through delivery of the service and to manage and limit risks that could result from insufficient utility and warranty of the service in operation. SVT shall not be performed by the same resources that build the release. The contractor shall provide service validation and testing to include:
    1. Identify the SVT process owner and manager and ensure they are not involved with any of the RDM activities for the any release that is part of the service
    2. Ensure proper testing occurs for all changes released into the production environments.
    3. Create and validate test plans.
    4. Manage the test plans and test environments.
    5. Conduct tests.
    6. Verify the results.
    7. Communicate the results to stakeholders.
    8. Create test reports.
    9. Evaluate the test according to exit criteria.
    10. Conduct post-release testing to evaluate the change to ensure it delivers value to the business.
    11. Validate and communicate results of testing activities.
b. The contractor shall provide quality assurance and production control support to ensure change to the GSA IT Infrastructure and services are monitored, structured, and controlled and adhere to industry best practices. The contractor shall provide the following quality and production control services:
    1. Perform Quality Assurance (QA) monitoring and reporting on compliance with designated standards, processes, and procedures.
    2. Conduct QA reviews and postmortem analysis of work activities and project/product deliverables to identify areas for correction and opportunities for improvement.

3. Manage, optimize, and enhance infrastructure operations production support processes for production control management, compliance monitoring, and the reporting of the workflow processes associated with tactical infrastructure operations.

C.5.4.5 SUBTASK 5 - SERVICE ASSET AND CONFIGURATION MANAGEMENT (SACM) SUPPORT

The contractor shall provide Service Asset and Configuration Management (SACM) services to manage the full service lifecycle of GSA IT assets and configuration items to include the following:

a. Develop and maintain a forward-looking SACM strategy and roadmap to mature GSA IT's existing SACM program to achieve the following goals:
    1. Identify the SACM process owner and manager
    2. Support efficient and effective service management processes by providing accurate and timely configuration information that aids decision making (e.g., to authorize change and release and resolve incidents and problems faster).
    3. Ensure the integrity between business requirements and configuration items by maintaining an accurate and complete Configuration Management System.
    4. Improve overall service performance and optimize the costs and risks caused by poorly managed assets (e.g., service outages, correct license fees, and failed audits).
b. Develop a SACM Management Plan that shall detail how the contractor will provide service asset and configuration management services in an ITIL-based framework.
c. Develop well-defined SACM processes and procedures with roles and responsibilities. Establish process interfaces between SACM and other processes; in particular, Change Management, Release and Deployment Management, and Knowledge Management (incidents and problems). Perform regular reviews of SACM processes, procedures, and associated techniques and methods to ensure continuous process improvement.
d. Establish procedures for auditing and verifying the accuracy of service assets and configuration items, adherence to SACM processes, and identifying process deficiencies. Audit and verify accuracy of service assets and configuration items and report deficiencies. Provide deficiency reports and recommendations on the steps to be taken to address the issues identified.
e. Establish appropriate authorization controls for modifying configuration items and verify compliance with software licensing. Develop procedures for establishing configuration baselines as reference points for rebuilds and provide ability to revert to stable configuration states.
f. Provide support for managing maintenance procurement activities, asset inventory control (including hardware and software license attributes), hardware and software asset lifecycle planning and management (e.g., timing of asset refresh, asset disposition), and software version management, and identify opportunities for refresh or insertion of technology.

g. Manage lifecycle of all assets from identification, requisition ordering, inventory, installation, and maintenance to disposal. Update asset records related to all approved change activities (e.g., Install, Move, Add, Change (IMAC) activities, break/fix activities, and change management).
h. Develop, maintain, and update an Equipment Spares Inventory Management Plan and spare inventory according to Section F, including recommendations on appropriate levels of spares for each equipment type at each Government facility sufficient to support the specified service levels and availability requirements.
i. Identify, document, and report license compliance issues by end users and recommend solutions to resolve issues. Manage and perform audits and reconcile the number of software licenses to the number of installs.
j. Manage and maintain the Configuration Management System (CMS) within the EITM system to include a logical model of the IT Service Areas' devices and their relationships by identifying, controlling, maintaining and verifying installed hardware, software, and documentation (e.g., maintenance contracts, SLA documents, etc.). The CMS shall account for all IT assets and provide accurate information on IT Service Area components and configurations and provide a sound basis for incident, problem, change, and release management and to verify configuration records against the infrastructure and correct any exceptions.
k. Work with the EITM System team to define and configure SACM capability.
l. Evaluate existing SACM systems and the design, implementation, and management of new and improved systems for efficiency and effectiveness.
m. Recommend key performance indicators and critical success factors that align SACM with GSA business needs to create a customer-focused IT delivery environment.
n. Provide reports, including management reports, configuration item analysis reports, and asset inventory reports.
o. Ensure all data relating to SACM is available to the Government when required.
p. Perform annual physical inventory of GSA IT assets in accordance with GSA policies.

SACM may cover non-IT assets, work products used to develop the services, and configuration items required to support the service that are not formally classified as assets. The scope covers interfaces to internal and external service providers where there are assets and configuration items that need to be controlled, e.g., shared assets.

The contractor shall develop a SACM Management Plan which will include SOPs, a SACM Strategy and Roadmap, an Annual Physical Asset Inventory Plan with Schedule, and outline the delivery of SACM Deficiency Reports as stated in Section F.

C.5.5 TASK 5 – PROVIDE SERVICE OPERATIONS MANAGEMENT

The contractor shall provide service operations management of the GSA IT infrastructure to maintain ongoing service operations stability while allowing for changes in design, scope, scale of the services, and service levels with minimal disruption to service delivery.

The contractor shall deploy robust, end-to-end operational practices and shall execute and manage the lifecycle of the following operational-level activities in a manner consistent with the ITSM framework:

a. Request Fulfillment
b. Incident Management
c. Problem Management
d. Access Management
e. Event Management

C.5.5.1 SUBTASK 1 - PROVIDE ENTERPRISE IT SERVICE DESK (EITSD) SUPPORT

The EITSD provides support to users of GSA's internal infrastructure as well as applications and systems owned by various GSA Service and Staff Officers. The EITSD is the single point of contact for GSA end-users and customers to report incidents, submit requests, seek advice, and register complaints about GSA's IT infrastructure, applications, and programs supported in the environment. The EITSD also provides an interface for users to other service management functions, such as change management, problem management, configuration management, and release management.

The EITSD shall be located in contractor's facilities. The contractor shall utilize pre-established geographically separated service desks with both the primary and failover service desk facilities located within the CONUS. The EITSD must be survivable and diverse such that the contractor can ensure continual operations in the event of a power outage, man-made or natural disaster. The EITSD should maximize synergy with the EIOC. The contractor shall provide a full description of the contractor's EITSD solution, to include but not limited to, facility, equipment and support systems redundancy, floor plan, total square footage, and any ATO that may be leveraged. The EITSD data provided shall enable the Government to clearly determine the contractor's ability to effectively manage and deliver service desk operations. The contractor's EITSD solution shall be subject to Government site survey and verification. The contractor shall provide an EITSD solution with the following minimum capabilities:

a. Responsive, reliable, and consistent service delivery 24 hours a day, seven days a week, 365 days a year (24/7/365) regardless of user location. Tier 1 and Tier 2 consolidated EITSD services in accordance with ITIL best practices.
b. Contractor-furnished and equipped service desk facilities (primary and failover) that are geographically separated and located in the continental United States (CONUS).
c. Contractor-furnished facilities meeting security criteria and ATO necessary to obtain connectivity to GSA.
d. Multiple alternative communications channels, including voice, voicemail, e-mail, web chat, Short Messaging Service (SMS), collaboration tools, and internet/intranet. Voice Communications Services that provide dynamic call routing, auto-attendant and call back, and the ability to post ad hoc outbound notifications for outages within minutes. The Interactive Voice System must allow for a prompt exit from the system and live communication with a service desk agent.

e. Demonstrated utilization of ITSM processes and industry best practices for customer service.
f. Processes that demonstrate service desk cradle-to-grave ownership for all service desk contacts from inception to closure, regardless of whether they are closed at the first level or passed to another service management group for resolution.
g. Demonstrated use of automated processes, remote device and software management technologies, self-help and self-healing options, and detailed, searchable knowledge bases that increase first level resolution at the service desk and minimize incident escalations.
h. Provides channels for proactively communicating information to customers. This information should include details of current system outages, applications issues, and network performance issues, and might include known issues that are likely to cause future problems or service interruptions, forthcoming changes, forthcoming releases of software and maintenance activities.
i. Prompt and proficient call response, trained, qualified and cleared technical personnel, clear and courteous communications (English), and timely incident resolution, escalation as needed, and closeout.
    1. All GSA customers have a single point of contact for each incident and Service Request and resulting Service Desk Ticket.
    2. All GSA customers receive appropriate, prompt, and responsive support.
j. Support services that are responsive to the time-sensitive needs of executives, to include prompt referrals to local IT support service.
k. User community easy access to a knowledge base to facilitate self-help and training resources for common IT problems/requests.
l. A full archive of service desk status and trouble ticket tracking information for the duration of the contract.
m. A managed, readily accessible, and actionable collection of recommendations for infrastructure and/or service improvements based on monitoring and identifying trends experienced at the service desk.
n. Utilize the Enterprise IT Services Dashboard (C.5.3.8) to reduce reporting time on service desk metrics and analytics.

The contractor shall operate the EITSD as the enterprise-wide single point of contact (SPOC) for providing end-to-end responsibility for responding to and managing all end-user calls for incident and service request support. The contractor shall provide all aspects of end-user support through the SPOC service desk, followed by a desk-side support capability for those incidents and service requests that cannot be resolved/completed remotely.

The EITSD shall receive, coordinate, record, respond to, track, monitor, diagnose, resolve or escalate and manage all incidents and service requests. The contractor shall resolve incidents and service requests at the service desk level to the maximum extent practical. The contractor shall refer or escalate incidents and service requests to more-specialized entities for resolution if the incidents or Service Requests cannot be resolved at the service desk level.

The EITSD shall manage the entire incident and service request process and assume “cradle-to-grave” ownership of end-user issues through ticket closure. This shall include acceptance of user calls, chats, and emails, ticket creation, centralized queue management, and tracking, Tier 1 and 2 first-level resolution and/or escalation, follow-up with users and Tier 2 Deskside services as needed (see Section C.5.5.2) to expedite and confirm resolution, root cause identification, and ticket closure.

The contractor shall utilize the “parent” (i.e., the initial Service Desk Ticket) in reporting performance and determining the number of tickets being processed and counted toward the contractor’s level of effort for any particular period. The contractor shall identify, manage, monitor, and report on all “child” tickets, work orders, etc. required in order to resolve the "parent" ticket.

The contractor shall utilize GSA’s ServiceNow Cloud-Based Enterprise Edition Service Management Suite (EITM System) provided as GFP as the service desk platform. The contractor may augment the system with additional modules, APIs and licenses if approved by the Government throughout performance of this TO. The contractor shall maintain the knowledge base to support the resolution of incidents and service requests.

The contractor shall implement and maintain Self-Help support capabilities that enable end-users to perform self-service including incident and service request status checking, password management and resets, a searchable knowledge base that includes self-help features such as Frequently Asked Questions (FAQ) and Questions and Answers (Q&A), common solutions and how-to instructions, connectivity instructions for teleworkers, search for service desk application support, and help tools (to include chat features).

The contractor shall support Government-furnished hardware to the device level and personal equipment to the connection level, i.e., the contractor shall make a "best effort" to assist personnel using personal equipment. Specific support shall be provided to assist users in installing and configuring remote access clients on personal equipment being used to access GSA internal and cloud-based resources and the installation of personal printers to government-furnished devices.

The EITSD shall provide enhanced executive level support for specifically designated senior executives and their immediate support staff via a Very Important Person (VIP) Hotline. For incidents related to GSA-designated executive users, the EITSD shall attempt to resolve on first contact and escalate by warm handoff to Deskside support or more-specialized entities for resolution.

The EITSD shall provide Tier 1 application support for GSA acquisition, financial, human resource, and administrative applications as follows. The contractor is required to maintain the necessary service desk knowledge, skills, and abilities to ensure continuity of services post-transition and to effectively support GSA applications for the life of the TO.

a. The contractor shall provide Tier 1 Financial, Human Resource, and Administrative Application support 0730 - 1930 Eastern Time (ET), Monday through Friday, except Federal holidays. The contractor shall provide extended hours and weekend support during fiscal year-end (last week in September through the third week in October).

b. The contractor shall provide Tier 1 Acquisition Application support between 0800 - 1900. ET, Monday through Friday, except Federal holidays.

The contractor shall provide Tier 0 support for GSA components, systems, and support applications that are not subject to coverage by the EITSD (for example, PBS (Public Building Service) National Applications support or Building Management). Areas not subject to EITSD coverage may require Automatic Call Distribution automated routing, warm handoffs, referrals, or ticket creation and routing to other help desks.

The contractor shall support the EITSD shared services environment and provide mechanisms for warm handoffs between help desks, managing shared ticket queues, and coordinating service activities among the different help desks. These services often involve a separate contact number and support personnel, including contractor and Government application subject matter experts (SMEs). Additional service fulfillment or support organizations are likely to be added over the course of the TO.

The EITSD shall work in conjunction with the EIOC to provide redundant coverage of all alarmed systems, e.g., communications links, communications routers, environmental systems, in order to detect and resolve outages. The contractor shall develop and implement a design that ensures both the EITSD and EIOC receive notification of an alarm simultaneously. In addition, the EIOC and EITSD shall provide failover alarm capability, i.e., in the event of failure at one location, the other location shall provide the alarm monitoring capability. An EITSD ticket shall be automatically generated upon detection of an alarm.

Following a major service incident or service outage, the contractor shall devlop Incident Reports and Root Cause Analysis Reports as referenced in Section F.

C.5.5.2 SUBTASK 2 - PROVIDE DESKSIDE SERVICES

The contractor shall provide Tier 2 Deskside touch support services in support of the full lifecycle activities associated with provisioning, operational logistics, installation, configuration, break/fix management of end-user computing devices and phones, and the LAN at GSA locations throughout the U.S., Europe, Puerto Rico, and Asia.

In performance of this task, the contractor shall:

a. Provide responsive, local, Deskside services to all on-site users to troubleshoot, diagnose, and resolve incidents and problems, and fulfill requests that require touch support that cannot be resolved at the first level by the EITSD.
b. Ensure all GSA customers receive appropriate, prompt, and responsive Deskside support services, equivalent services for GSA customers are provided regardless of location; a more efficient and cost-effective local support service delivery model; and a high level of end-user satisfaction with services are provided, demonstrated, and documented through customer satisfaction surveys.
c. Provide Deskside IT services that appropriately respond to the time-sensitive needs of VIPs and executives, to include prompt responses to Tier 1 Service Desk escalations.

   Provide Deskside support personnel on-site at all ROBs and GSA HQ during the core business hours as listed in Attachment O.

d. Provide full support remotely for field offices and local users located outside of ROBs and HQ as shown in Section J, Attachment L. This includes dispatching technical support personnel to field offices between normal business hours of 0600 and 1800 local time.
e. Provide a contractor solution that minimizes response times and costs for all OCONUS Deskside support that includes:
    1. A mix of onsite and offsite technical resources to support core business hours and responsive on-call support outside of core business hours.
    2. SLAs for response times, incident resolution, and request fulfillment.
        i. Europe Operations:
            a. Provide responsive and reliable dispatch support during core business hours of 0700 - 1700 local time.
            b. Constraint: The Government will not provide Status of Forces Agreement (SOFA) sponsorship.
        ii. Hawaii Operations:
            a. Provide responsive and reliable dispatch support during core business hours of 0700 - 1700 local time.
            b. The contractor must acquire base access through Rapid Gate Program.
        iii. Asia Operations:
            a. Provide on-site deskside support during core business hours of 0800 - 1700 local time.
            b. Asia operations currently support Japan, Korea, Guam, and Singapore.
            c. SOFA clauses will be included in the TO to allow for unescorted base access (Section H.8.1).
        iv. Puerto Rico and the Virgin Islands Operations:
            a. Provide responsive and reliable dispatch support during core business hours of 0600 - 1800 local time.
f. Provide Deskside support after normal business hours via on-call personnel.
g. Utilize the existing EITM system to fully document all work performed in a timely manner.
h. Provide break/fix, asset inventory, spares/parts management, desktop administration, remote access, “smart hands” touch support for all other support teams (except at GSA designated Data Centers), troubleshooting and upgrading of mobile devices, and security services for all end-user devices.
i. Provide support to include infrastructure support services from the local router down through and including all the hardware, software and cabling required to support the data, voice, and video communications needs of users. The contractor shall coordinate support with other service providers and carriers to include providing facilities escorts to other service providers.
j. Present topics to the CCB for approval.

k. Provide Deskside services to include both hardware and software and include:

1. Large and small scale IMACs to include regional technology refreshes
2. Operational monitoring
3. Problem determination and resolution
4. Tier 2 technical support
5. Break/fix services
6. System and office productivity software deployment and management
7. Remote access service support
8. Light training and testing support
9. Server operations and administration
10. Backup and restore
11. Cable management
12. Asset and inventory management
13. Copying and preserving data for litigation hold cases
14. Toner/Ink management and replenishment and Printer Repair. The contractor shall provide toner management and replenishment for printing devices, and printer repairs when cost advantageous to the Government. For printers (including large format printers) that are not leased or supported under separate maintenance contract, the contractor will be responsible for installing fuser kits, transfer kits, and rollers when such effort can be accomplished without requiring board-level or connector-level disassembly of the printer's internal components. In remote locations where there is no local onsite support, toner will be shipped to the site and customers will assist in installing the toner if they have the appropriate technical knowledge. On occasion, the contractor will have to dispatch a technician to change toner.

l. Provide IT technical support for local special events, conferences, and meetings.

m. Provide on-site Video Teleconferencing (VTC), Audio/Visual and Telepresence support to include conference rooms, training rooms, auditoriums, senior leadership offices and workspaces, and Telepresence rooms. Support includes training end-users how to use equipment, equipment set-up, starting meetings, and troubleshooting issues. Deskside services also functions as the Video Communications Services Tier 2 technical experts and smart hands in the regions.

1. In some GSA Regions, GSA shares space with other Federal agencies. As a result, when VTC support is needed in some of the conference rooms, Deskside support shall bring in and set up a portable GFE-provided VTC cart so that a successful meeting can be accomplished. For almost every large VTC meeting held, Deskside support is involved in providing support to ensure that the VTC meeting begins successfully. In some GSA Regions where there are non-standard VTC units such as desktop camera connectivity, Deskside support shall be able to troubleshoot and connect these devices to ensure that the conference call begins successfully.

2. Provide Deskside services to support the GSA Central Office HQ Auditorium, Conference Center, and 200 plus conference rooms equipped with VTC, A/V, and telepresence equipment. The large Conference Center is used for large events and meetings (e.g., town hall meetings) where video is used to connect to other conference rooms across the U.S. Deskside services is responsible for providing all support for these rooms including coordinating the setup of a video conference bridge, meeting with customers to gather their requirements and explain the capabilities/restrictions of the Conference Center, ensuring the right cameras are operating during the meeting, and ensuring that meetings go successfully using the technology available in the rooms. Most conference rooms have built in VTC equipment, but some smaller rooms require the use portable GFE VTC carts.

n. Provide on-site support for a storefront solution that is established in all GSA ROBs and HQ. The storefront solution, known as the IT Insider Store, is a walk up location whereby customers can walk in and obtain assistance with IT issues or ask questions and get quick answers on "How do I?" type questions. The storefronts also stocks loaner laptops where customers can pick up one when needed for the day.

o. Provide technical support for small and large computer deployments, to include support for distributed computing hardware resources, including networked and non-networked personal computer (PC) systems on the distributed computing environment personal/local printers, scanners and other peripherals; and tablet computers and other similar devices.

p. Provide facilities-related services to include cable installation in locations with existing access, termination, testing, and maintenance; installs, removes, maintains, consolidates and enhances fiber optic/twisted pair/coaxial cabling to support the enterprise infrastructure; and servicing of wiring closets and related contents. The Contractor must survey and supply the bill of material for the project, provide all materials and equipment required to complete the project, manage the full lifecycle of the cable project, and ensures personnel assigned to the project have the necessary certifications to meet project requirements and GSA standards (i.e. GSA TDDG, BICSI, etc.).

q. Provide dispatch support to GSA Enhanced Check-out (GECO) stores for equipment repair/replacements.

r. Provide regional on-site and dispatched infrastructure support for PBS Building Management Control (BMC) systems. These services include maintenance, break/fix, and refresh support of the BMC workstations, laptops, and kiosk workstations; regional infrastructure support including "smart hands" for installation, maintenance, repair, and troubleshooting server, switches, and routers; and cable installation and configurations.

s. Provide IT support for pilot projects and shared services. GSA's Central Office HQ and several ROBs currently support the pilot Workplace Initiative Program that exists whereby other Federal agencies may schedule to come in to the GSA HQ location and temporarily work in the "open concept" workspace to see if this type of working conditions/arrangement will work for them at their location. There is a limited amount of workspaces set aside for other agencies to book. When they arrive, Deskside support meets with the customer, assists them with connecting to the GSA Guest Wireless network, and provides instructions on how to print to dedicated printers in the area. The contractor shall maintain an inventory of loaner laptops with local accounts that can be

provisioned if customers do not bring their own device. This pilot may be implemented in other GSA Regions in the near future. In addition, GSA requires support for any other innovation pilot projects that would require the support of IT technical staff.

t. Provide Smart Hands Support – Some GSA Regions do not have personnel available to perform the "touch" support required. Deskside support performs "smart hands" tasks at the direction of other teams such as: infrastructure hardware installations, configuration, and decommissioning; assisted troubleshooting, reboots, and physically power cycling equipment; asset location and verifications; and visual inspections of systems. Deskside support shall act as the "touch" support for these other teams to accomplish their mission and get the equipment back up and running, possibly after normal hours of operation.

u. The contractor shall report real time Deskside support operational and performance status through the Enterprise IT Services Dashboard.

C.5.5.3 SUBTASK 3 - ELECTRONIC MESSAGING AND COLLABORATION SERVICES

GSA requires full administrative support of the Google Suite of Applications available in the Google GovCloud. This suite includes, but is not limited to, Google mail, calendar and groups. In addition, the contractor shall provide support for legal requests that GSA is required to support to the GSA Legal Departments, Freedom of Information Act (FOIA) requests, and Inspector General (IG) requests.

The contractor shall provide the following support to GSA and to other Government departments, agencies, boards, and commissions:

a. Google Applications (Apps)
    1. Google mail
        i. New Hire Request / Individual Mailbox (update GSA's internal directory service (GCIMS), Netiq, Google)
        ii. Creating an email alias address of the Google mailbox
        iii. Username Changes
        iv. Export/import of Google account data
        v. Enable/disable out of office on behalf of users
        vi. Google account delegation
    2. Calendar (User Calendar/Shared Resource)
        i. Create and delete calendars
        ii. Create and delete resources
        iii. Delegate users to shared calendar and resources
        iv. Transfer ownership of a shared calendar
        v. Export calendar data
    3. Google Group
        i. Google Group management (create, update, delete)
        ii. Bulk Group membership update

iii. Creating an email alias address of the Google Group mailbox

4. Shared Mailbox
   i. Shared Mailbox (create, delegate, delete)
5. Google Sites
   i. Provision Google Sites
   ii. Manage Google Site Access Control Lists
6. Miscellaneous
   i. Google Active Directory Sync application and server support
   ii. Manage Gkey.gsa.gov application and server support. Application is an .asp application running on IIS that allows users to update Google passwords.
   iii. Assist users with "bulk" mailings.
   iv. Google Doc transfer and account deletion for departed users.
   v. Support testing in GSA's Google sandbox environment (test.gsa.gov).
   vi. Support the GSA enterprise FAX environment currently running Esker Fax.
   vii. Manage issues with the service delivery provider (Google); this includes management of cases and providing status update when there are service delivery issues.
   viii. Manage support tickets with Google using the Enterprise Google Apps service portal.
   ix. Manage Google Apps domain for gsa.gov (audit report, log search, enable/disable Google services, add/remove/update Google admins, etc.)
   x. Supporting the following Google services:
      a. Mail, Calendar, Documents, Sheets, Drive, Groups, Plus, Hangouts, Sites as well as other non-core Google Apps such as Analytics.
   xi. Document and update Google Cpanel settings.
   xii. Change Release Board and CCB support.
   xiii. Adding domain alias to GSA.GOV.
   xiv. Use of the Google Apps APIs to automate administration and reporting tasks through scripting. This could include scripts to perform bulk updates to the gsa.gov Google domain (i.e., set default calendar access to all users' calendars). Languages may include Python, Java, etc.

b. Legal Requests
   1. Litigation (GSA Lawyers) Requests
      i. Placing users on litigation hold in Postini (migrating to Google Apps Vault).
      ii. Removing users from litigation hold in Postini.
      iii. Placing information in the Evidence Preservation Requests (EPR) internal

tracking database.

iv. Providing data in .pst and/or .mbx file format.

v. Loading data on Government-furnished media to hand over to Legal.

2. FOIA Requests
   i. Execute criteria searches in Postini, download data to .pst and/or .mbx file format.
   ii. Enter request information into EPR internal tracking database.
   iii. Upload data to Google drive or burn to Government-furnished media for delivery.
3. IG Requests
   i. Execute criteria searches in Postini, download data to .pst and/or .mbx file format.
   ii. Enter request information into EPR internal tracking database.
   iii. Upload data to Google drive for IG's office.
4. Congressional Requests
   i. Execute criteria searches in Postini, download data to .pst and/or .mbx file format.
   ii. Enter request information into EPR internal tracking database.
   iii. Download data to media for hand over to congressional representative.
5. Department of Justice (DOJ) Requests
   i. Execute criteria searches in Postini, download data to .pst and/or .mbx file format.
   ii. Enter request information into EPR internal tracking database.
   iii. Create current copy of user's mail file in .pst format.
   iv. Download data to media and hand over to DOJ representative.
6. Access to another User's "Mailfile" (Government Employee)
   i. Grant access to the requested users mailfile
7. Access to another User's "Mailfile" (Contractor)
   i. Grant access to the requested user's mail file.

c. Simple Mail Transfer Protocol (SMTP)
   1. Security
      i. Block requests - Postini/Google apps content manager and blocked sender lists.
      ii. Postini/smtp.gsa.gov [a/k/a agg]/mailgate/gmd log search for malware recipients.
      iii. FISMA questionnaire responses.
      iv. Update system security plan and controls.
      v. Security incident coordination with IT Security (e.g., spill incident, infection, etc.).

vi. Maintenance of email-related perimeter firewall exceptions.

2. Routing
   i. Changes to transport in postfix.
   ii. Org creation/adjustment/addition in Postini and Google Apps cPanel.
   iii. Routing rules/changes in Postini and Google Apps cPanel.
   iv. Routing rules in Google Apps.
   v. Additions to Mailgate hosts/domains/mail policies.
   vi. Mx/spf record creation using the Domain Name System (DNS) team.
   vii. Data Loss Prevention (DLP) rules in Google Apps cPanel.
3. Whitelisting
   i. Checking bounced messages for correct type of whitelisting.
   ii. From address, sending Internet Protocol (IP).
   iii. Postini IP Lock.
   iv. Sender Policy Framework (SPF) record addition.
   v. Managing Postini and Google Apps approved sender list.
   vi. Helping users to complete the whitelist exception request security form.
4. Internet Address Block Inbox
   i. User instruction on spam button and blocked sender list.
   ii. Check headers/logs/IP ownership/included URLs.
   iii. Forward to security for blocks determination.
5. SMTP Relays (smtp.gsa.gov)
   i. Patching/upgrading
   ii. Maintenance scripts
   iii. Heartbeat message origination
   iv. Red Hat Enterprise Linux (RHEL) 6 Migration
6. DLP Solution (Mailgate)
   i. Releasing False Positives from Social Security Number (SSN) Filter
   ii. Patch 4 deployment
   iii. Version 5.3.1 + upgrade
7. Postini
   i. Support/Test test.gsa.gov in Postini
   ii. Documentation and update of Postini settings
   iii. Synchronize information between Google Apps and Postini
   iv. Manage Postini all supported domains (audit report, log search, enable/disable services, add/remove/update Postini admins etc.)
   v. Postini sunsetting planning w/Google and ITSec
8. Delivery issues
   i. Message tracing across logs between mailgate/sgg/Postini

ii. Bounce message interpretation
iii. Mailgate message status verification
iv. Postini quarantine status verification

9. Working with non-GSA Mail admins
   i. Explanation of/writing of/correcting broken SPF records
   ii. Corrections for broken mx records
   iii. GSA application developer email education/configuration assistance

C.5.5.4 SUBTASK 4 - PROVIDE IDENTITY AND DIRECTORY MANAGEMENT SERVICES (IDMS)

The contractor shall provide an IDMS (create, change, delete user accounts, privileges, and roles) that includes management, administration, and support of Microsoft Active Directory (AD) domain structure. This shall include password management, directory synchronization, single sign-on (SSO) capabilities including the use of Security Assertion Markup Language (SAML) 2.0, user provisioning capabilities including those for privileged accounts, and electronic authentication and authorization for system access and transaction processing.

The contractor shall address data normalization and standardization of disparate directories as well as establishing rules of behavior for interacting with managed Directories.

The contractor shall be responsible for GSA AD Domain(s) DNS services, Dynamic Host Configuration Protocol (DHCP) authorizations, Group Policy management, schema extensions management, establishing security boundaries and contexts, managing Organizational Units, maintaining AD security policies, and setting group and user permissions structures.

The contractor shall provide access to the AD through a number of federation services. IDMS shall establish policies and procedures to address cleanup of rogue and/or orphaned objects within the domain.

The contractor shall manage encryption services to include hard disk (full disk) data at rest encryption, password encryption, and application of new authentication encryption technologies (to include strong authentication, Public Key Infrastructure (PKI)-level encryption with smart cards and/or tokens, Multifactor Authentication, and One Time passwords). This includes support of a PKI infrastructure and controls for supporting access and management services via service accounts.

The contractor shall maintain logs for daily performance management as well as for exception events and ad hoc event reporting as necessary; this logging should extend to application support Directory functionality such as PKI, single sign-on, or password management. The IDMS shall perform a review and analysis of the results and report findings for all critical AD-related functions, services, and security indicators.

The contractor shall utilize automation and role-based management to ensure availability of access and ensure continuity of services. The contractor shall provide highly available and geo-redundant active directory and supporting services and personnel.

Any proposed solution must include testing and deploying system enhancements to increase existing functionality, provide additional functionality, or perform functions in a more efficient manner (including through the use of cloud-based services).

C.5.5.5 SUBTASK 5 - PROVIDE DATA CENTER SUPPORT SERVICES

GSA IT currently operates a primary data center located at Stennis Space Center, Stennis, Mississippi, a secondary data center in Fort Worth, Texas, and GSA PBS data center with some secondary enterprise hardware in Chantilly, Virginia. It is anticipated by summer 2015, that GSA IT will have made a decision on a new secondary location that will need the same parallel support provided to the Stennis Data Center. Services may be required to move several existing locations (Fort Worth, Chantilly, HQ, and the National Capital Region (NCR) ROB enterprise computing infrastructure) to the new data center location. The data center office is also responsible for ensuring support oversight and process adherence within GSA IT Regional Infrastructure Closets across the enterprise.

As part of data center support, the contractor shall provide:

a. Onsite decommissioning support.
b. Smart Hands support (installation of cards, Small Form Factor Pluggables (SFP), etc.).
c. Rack management.
d. Data Center move support.
e. Inventory/asset management as referenced under SACM.
f. On-site support to RDM and SVT activities
g. Escorts to third-party vendor support personnel.
h. Shipping and receiving as coordinated with GSA.

C.5.5.6 SUBTASK 6 - PROVIDE SERVER AND STORAGE MANAGEMENT SERVICES

The contractor shall provide technical, administrative, and operational support services for GSA's server and storage infrastructure supporting the full lifecycle of server and storage deployment, operations, enhancements, and management across the GSA Enterprise for both physical and virtual devices.

The scope of this lifecycle support includes provisioning, configuration, hardening, administration, maintenance, upgrade, enhancement, monitoring, data protection, and management of GSA’s operational and application systems. Assets located in the Enterprise, but not at a core data center, shall be managed via remote access and/or in conjunction with Deskside support resources, these include services needing to stay localized or those services not yet consolidated within a core data center. This support includes the need for support of large or complex, project-based infrastructure build outs, expansions, and/or upgrades. These services will be based on solid offerings to include the following: unified availability, monitoring and reporting, performance management, incident management, and system management. Focus should include automation of routine and advanced tasks, of system changes and software deployments, and remediation of service disruptions or outages. The contractor shall exhibit the ability to staff diverse technical specialists able to respond quickly to the many variables and

conditions that accompany typical administration and enhancement efforts in rapidly changing or evolving technologies while providing practical, cost-efficient services.

GSA IT will own all server, data storage system, peripheral, and network hardware and software needed for managing critical business line infrastructure. During the period of performance of this TO, it is the Government's desire to migrate server and storage services to technologies that enhance efficiency, are robust, and are reliable to serve GSA IT stakeholders. Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) initiatives are two examples that may provide a framework that is more cost effective and can be adapted to meet the dynamic infrastructure and computing requirements of the GSA IT organization and stakeholders.

The contractor shall provide full lifecycle enterprise services for server, storage appliance, and associated infrastructure to include, but not limited to, architecture and design of server and storage solutions, enhancements, and upgrades, server project management, system builds, configurations; and provisioning as well as automation of such tasks and extending self-provisioning to customers within a well structured environment; operate, maintain, and manage the existing environment across multiple platforms, operating systems, and appliances; security monitoring and vulnerability remediation; data protection, including immediate recall, near line recovery and the transition away from off line recovery; COOP/DR availability to provide as a service where required; virtualization support and optimization; maintenance of hardware warranties and vendor support; tracking, evaluation, and presentation of developments in commercial services for implementation (e.g., cloud services, tools, techniques); and establishing policy, procedure, and management oversight of file and data management services (Home and Shared volumes/directories) in collaboration with the IDMS policies and procedures for authentication and authorization.

C.5.5.7 SUBTASK 7 - PROVIDE CRITICAL BUSINESS INFRASTRUCTURE SERVICES

The goal of critical business-line infrastructure support requirement is to provide timely and cost-efficient support services to stakeholders while testing and deploying 'new' system enhancements for the GSA business lines and support offices. GSA IT requires infrastructure management services at GSA locations (Government sites).

During the period of performance of this TO, it is the Government's desire to migrate critical infrastructure services to technologies that enhance efficiency, are robust, and are reliable to serve GSA IT stakeholders. Cloud initiatives, IaaS and PaaS, are two examples that may provide a framework that is more cost effective and can be adapted to meet the dynamic infrastructure and computing requirements of the GSA IT organization and stakeholders.

Critical business-line infrastructure support services include, but are not limited to, Server, Storage, and Network Tuning, System (server/storage and assistance with application) Optimization, System Replication, System COOP/DR support, Architecture and Planning for optimal performance, System Security, and Data Protection. These services will be based on solid offerings to include the following: unified Availability, Monitoring, and Reporting, Performance Management, incident Management, and System Management; providing these above and beyond what Server and Storage Management offers and focusing on maximum performance, end user experience, and uptime. Focus shall include automation of routine and advanced tasks, of system changes and software deployments, and remediation of service

disruptions or outages. Infrastructure for the purposes of critical business-line systems includes lifecycle management for standard servers, web hosting servers, and database servers providing these as pre-built platforms where appropriate, and with an emphasis toward moving all builds and processes toward platform-based systems.

These systems consist of Windows and non-Windows systems, and a multitude of hardware platforms. Any offering should adhere to methodologies provided as part of overall GSA IT management. Critical Business Infrastructure support shall build upon the foundation established within the Server and Storage Management offering, and utilization of tools, techniques, and methodologies shall be shared across the Server and Storage Management and Critical Business Infrastructure teams.

Refer to Section J, Attachment G for Critical Business Infrastructure Service Levels.

C.5.5.8 SUBTASK 8 - PROVIDE NETWORK OPERATIONS SERVICES

The contractor shall operate, maintain, and modernize the GSA network infrastructure. GSA's data network is critical to achieving the mission of the Agency. GSA IT currently manages its own MPLS network, which consists of hundreds of circuits, multiple routing protocols (Enhanced Interior Gateway Routing Protocol (EIGRP), Multi-Protocol-Border Gateway Protocol (MP-BGP), Open Shortest Path First (OSPF)) and multiple internet connections.

The contractor shall provide highly innovative approaches to managing the large and complex GSA network infrastructure. The contractor shall provide expertise in routing protocols, network management, and element management tools such as CiscoWorks, HP Openview and Solarwinds in order to effectively operate the network and troubleshoot complex network issues that arise.

One of GSA IT's objectives is to modernize its network infrastructure by transitioning to a technical framework that enables rapid response to emerging technology trends and complex Government requirements. The contractor shall assist GSA IT in modernizing the network infrastructure by assisting with the following:

a. Redesigning, streamlining, and replacing T1 circuits with IPSEC VPN tunnels or Ethernet.
b. Transitioning to a fully managed network solution to include management of routers and switches.
c. Implementing a SDN capable network.
d. Leveraging cloud integration with major cloud vendors, e.g., Amazon Web Services (AWS) and Salesforce.
e. Implementing a full mesh to optimize the end-user experience.
f. Real-time monitoring of performance and network utilization.
g. Instituting an expanded, more systematic use of SLRs and enforceable performance measures.

The contractor shall provide performance management services associated with tuning the GSA enterprise network for optimal performance. The contractor shall collect performance metrics and monitor the performance of critical components to include, but not limited to: availability/uptime, response time, end-to-end throughput, bandwidth utilization, load balancing, and potential error conditions. The contractor shall report on availability, at the component level,

on a monthly basis. This includes Performance Analysis and Performance Reporting as stated below:

a. Performance Analysis**.** The contractor shall analyze performance metrics collected by automated monitoring to track usage and trends. The contractor shall provide recommendations to maintain or improve performance.
b. Performance Reporting**.** The contractor shall prepare and submit a Performance Report that charts the actual performance of the enterprise-wide environment within the reporting period against specific thresholds.

Additionally, the contractor shall perform the following performance planning related items:

a. Develop, document and maintain standards and procedures manuals, and performance management procedures that meet GSA's requirements
b. Perform network component tuning to maintain optimum performance in accordance with change management procedures
c. Provide regular monitoring and reporting of performance, utilization, and efficiency
d. Proactively evaluate, identify and recommend configurations or changes to configurations that will enhance performance

The contractor shall deliver the following plans according to Section F:

a. Network Performance Plan - The plan shall include realistic milestones and in depth analysis. Implementation of the Network Performance Plan shall start three months after Government approval of the Network Performance Plan.
b. Network Modernization Plan - The plan shall include realistic milestones and in depth analysis. Implementation of Modernization plan shall start three months after Government approval of the Network Modernization Plan
c. Network Capacity Plan - The plan shall include realistic milestones and in depth analysis. Implementation of capacity tracking must start six months after PS. The capacity plan shall provide for quarterly capacity and monthly performance reports and include network capacity and bandwidth utilization for all ROB locations, all LAN/WAN connection (MPLS), all Internet MTIPs connections, VPN connections, and all Field Office connections. The capacity plan shall also include WIFI utilization and other capacity related metrics.

The contractor shall perform the following operations and maintenance tasks:

a. Routers and switches manage, support and maintain GSA's Internet connections (24/7/365)
b. Design, configure EIGRP/OSPF/BGP/MPLS to achieve best optimal internet/intranet routing path selections for ROB, Field Office, and VPN users in normal and failover operating modes
c. Configure load balancers to deliver automated load balancing / fail over support for production processing of GSA IT applications
d. Recommend WAN / LAN / WiFi / VPN / Identity Services Engine (ISE) Firewall technical solutions based on industry best practices

e. Support, Operate, Manage and Maintain LAN / WAN / WiFi / ISE connectivity including Layer 3 Multicast contained in the GSA IT network infrastructure
f. Develop and document network administration requirements and policies
g. Develop and document procedures for administration that meet requirements and adhere to defined policies and procedures
h. Perform day-to-day network operations and administration activities
i. Network systems management and troubleshooting (e.g., performance, problem, change and capacity monitoring)
j. Overall Bandwidth management for the GSA network
k. Protocol usage statistics (e.g., identify top talkers by protocol)
l. Work with public carriers and other circuit providers to perform any operations activities (e.g., provisioning, problem management
m. Manage and maintain all Network devices in the computing environment including routers, switches, Access Point (AP) devices, WAN Optimization, ISE, Load Balancers, and other network hardware components.
n. Perform operating system upgrades on all routers, switches, AP devices, WAN Optimization, ISE, Load Balancers, and other network hardware components in the GSA computing environment.
o. Manage router configurations, Internet Protocol (IP) addresses and related services (e.g., DNS / DHCP / Access Control System (ACS))
p. Physical (e.g., equipment) and logical (e.g., IP address change) IMACs
q. Manage network devices in accordance with GSA IT policies (including security oversight and change management policies)
r. Maintain IP addressing schemes, router configurations, routing tables, and VPN configurations
s. Manage user accounts as needed for access and maintaining network resources (e.g. logon user-id and password maintenance)
t. Maintain and provide audit information including access, general logs and application logs in accordance with the GSA security policies
u. Ensure that network administration activities are coordinated through defined change management processes
v. Develop and document requirements and policies for network monitoring and problem management
w. Develop and document network monitoring and problem management procedures, including escalation thresholds that meet requirements and adhere to defined policies
x. Provide and recommend network management tools to efficiently manage the GSA network
y. Manage and implement tools for monitoring network devices and traffic. Use automated processes via network management tools to manage and maintain networking devices (e.g. routers, switches, AP devices)

z. Implement measures for proactive monitoring and self-healing capabilities to limit network outages

aa. Monitor network connections in accordance with the EIOC quality assurance guidelines and the carrier Service Level Agreements

bb. Identify network problems and resolve in accordance incident and Problem Management Services, policies, procedures and Service Level Requirements

cc. Perform maintenance and problem resolution activities onsite at GSA CONUS and OCONUS facilities; and

dd. Coordinate resolution of circuit problems with third parties, including public carriers, Internet Service Provider, and City/County affiliates

ee. Setup, configure, architect, manage, and maintain geographic load balancing for critical applications identified by the Government.

ff. VPN Services – The contractor shall provide VPN services. VPN services include the provision, monitoring, and management of methods for securely connecting to the Network and Data Center Computing Services environment.

gg. Coordinate provisioning of broadband connections with GSA field offices.

hh. Setup, install, configure and manage broadband connects on the GSA network.

ii. Network Tools Management

1. Write scripts to push commands to routers, switches, load balancers and AP devices. Write scripts to manage routers, switches, load balancers and AP device configurations.
2. Develop automated processes to perform connectivity testing and validation for maintenance events and on-going operations or major cut-over.

jj. WAN Optimization

1. Provide operations and maintenance support for WAN optimization appliances deployed throughout GSA. Deliver monthly metric regarding WAN optimization performance and recommend optimized solutions for bandwidth efficiency usage.

kk. Data Center Network

1. Manage and maintain current GSA data center network infrastructure which supports all mission essential business applications, as well as recommend solutions for a hybrid private/public data center.
2. Recommend use-cases for leveraging the capabilities of SDN at the data center.

ll. Building Systems Network

1. Design, implement and maintain the Building Systems Network (BSN)
2. Provide BSN architecture expertise and recommendations
3. Deploy network equipment (switches, routers) to sites in a timely manner
4. Resolve network hardware issues
5. Provide IP connectivity
6. Port configurations
7. Real time 24/7/365 support for troubleshooting connectivity issues and outages

8. Manage an inventory of network equipment to support BMC projects
9. Provide critical, real time support for system integrations

mm. Identity Services Engine

1. Provide support for operations, maintenance, and troubleshooting for ISE. Document ISE deployment in the GSA infrastructure.
2. Implement network configuration and integration with Mobile Device Management (MDM) to provide a secure Bring Your Own Device infrastructure

nn. ACS -Manage, maintain, and support ACS Wi-Fi user name/password management.

oo. Asynchronous Transfer Mode (ATM) - Manage and maintain backup ATM network for regional office locations.

pp. Federal Protective Service (FPS) Environment - Configure, manage, and monitor ATM WAN Virtual Path Identifier (VPI)/Virtual Circuit Identifier (VCI) on Cisco MGX ATM switches supporting frame-relay users

Refer to Section J Attachment G for Network Operation Service Levels.

C.5.5.9 - SUBTASK 9 - PROVIDE ENTERPRISE INFRASTRUCTURE OPERATIONS CENTERS (EIOC) SUPPORT

The contractor shall provide EIOC support to continuously monitor and manage the health and performance of GSA IT infrastructure and services to include the following:

a. Operate and maintain a 24/7/365 EIOC. The EIOC shall be located in contractor's facilities within the CONUS and must be survivable and diverse such that the contractor can ensure continual operations in the event of a power outage, man-made or natural disaster. The EIOC should maximize synergy with the EITSD. The contractor shall provide a full description of the contractor's EIOC solution, to include but not limited to, facility, equipment and support systems redundancy, floor plan, total square footage. The EIOC data provided shall enable the Government to clearly determine the contractor's ability to effectively manage and control infrastructure operations. The contractor's EIOC solution shall be subject to Government site survey and verification.
b. Perform monitoring and intervention activities, including detection, isolation, and resolution of issues affecting service availability and performance.
c. Perform proactive and reactive troubleshooting.
d. Perform timely escalation and notification of service problems and outages.
e. Maintain an accurate list of Circuit Points of Contact for escalations and outages.
f. Coordinate with service providers and carriers to restore services.
g. Operate and maintain network management tools to automate and improve service/component monitoring, problem identification, problem resolution, performance analysis, and configuration management.
h. Report real time operational health of critical IT services such as the network, voice, video and critical business-line infrastructure through the Enterprise IT Services Dashboard.

i. Deliver EIOC Escalation Procedures with designated points of contact within the first 60 days after Project Start. Escalation procedures must take into consideration the diverse environment and impact to GSA users and service delivery as well impact to tenants in High Impact Buildings. The information shall be updated and reissued upon any change to the contractor's escalation procedures or contacts and shall be provided to the Government within 24 hours of the change implementation. The procedures shall include a description of the circumstances under which issues shall be escalated with associated timelines.

The contractor shall perform proactive and reactive monitoring across the full spectrum of GSA IT technologies and services to include:

a. Network telecommunications circuits GSA IT technologies and services
b. Network switching and routing equipment for wired and wireless devices
c. IT infrastructure servers (e.g., file, print, domain name service, etc.)
d. Voice over Internet protocol (VoIP) components
e. VTC components
f. Video streaming components
g. Environmental monitoring systems
h. Power management devices (e.g., uninterruptable power supply, etc.)
i. Servers for critical business-line infrastructure
j. Building monitoring and control systems (these systems may be located in buildings where there is no GSA users present)
k. Energy metering systems
l. Physical access control systems
m. Infrastructure back-office applications

GSA IT currently monitors individual components of the infrastructure. Service monitoring has been implemented in some cases at a rudimentary level. The contractor shall transition to a holistic and integrated service monitoring and reporting model to provide more useful monitoring status information to end-users and GSA application owners. The contractor shall:

a. Provide a transformative monitoring approach that is holistic and capable of assessing the operational status of critical applications and IT services.
b. Provide performance baseline metrics for critical services and the network.
c. Design the monitoring solution to be scalable and dynamic to allow for adding services and components during the contract period of performance.
d. Implement a services-based monitoring approach for critical IT services such as Voice Over IP, VPN, and business applications.
e. Implement a solution to assess operational status of key IT services and to baseline key IT services through the use of synthetic transactions.
f. Increase the use of automation (e.g. fault correlation, ticket generation, self -healing scripts, etc.).

g. Deliver an EIOC Transformation Plan within six months post-award. The plan shall include realistic milestone and in depth analysis for transforming EIOC operations. Implementation of transformation plan shall start three months after Government approval of the EIOC Transformation Plan.

C.5.5.10 SUBTASK 10 - PROVIDE UNIFIED COMMUNICATIONS SERVICES

The contractor shall operate, maintain and transform GSA's voice, video, and web conferencing communications services infrastructure by providing full lifecycle engineering support resulting in solutions that achieve the following objectives:

a. Secure – ensure solutions comply with all applicable security specifications.
b. Effective – ensure positive customer experience by delivering high performing solutions.
c. Responsive – ensure solutions meet customer expectations in terms of being proper and timely.
d. Complete – ensure reports/documentation are comprehensive, accurate, and up-to-date.
e. Efficient – achieve operational and cost efficiencies.

GSA IT Voice and Video Communications Division consists of four functional areas these functional area's will be referred as systems if not called out by name:

a. Unified Communications
b. Legacy Telecommunications to include Call Centers
c. Web Conferencing
d. Video Communication Services

GSA IT Unified Communications System strives to be the most Innovative, Intuitive, and Integrated (I3) solution that can be deployed to meet the communications needs of GSA employees. In support of these efforts, the contractor shall provide a best-in-class service to maintain these systems, recommend improvements and enhancements to the Government, and execute successful upgrades and transitions when approved and requested by the Government.

The contractor shall:

a. Provide optimization support service including, but not limited to software, performance engineering and optimization and knowledge transfer and mentoring on service modules in support of CISCO and Avaya's Family of Communications products.
b. Provide Design Consultation
c. Provide Systems Change Support for deployment-related hardware, software, or configuration events such as:
    1. Evaluating the potential impact of proposed scheduled changes
    2. Review implementation procedures
    3. Assist in resolving network hardware, software and configuration issues
d. The contractor shall assist GSA with optimizing services on GSA's large and complex network. This includes assisting with engineering support, routing optimization, VPN tunnel and engineering support. Assessing network operations to identify and analyze

critical performance indicators and operation gaps that can pose significant risk to the health of the Unified Communications, Video and Avaya systems

e. Provide systems change support for deployment-related hardware, software, or configuration events:
    1. By evaluating potential impact of proposed scheduled changes
    2. Review implementation procedures
    3. Assist in resolving network hardware, software and configuration issues
f. Provide systems improvement plan support, which may include:
    1. Quarterly improvement plans incorporating recommendations from annual assessment.
g. Evaluate the capabilities of GSA's currently deployed software levels on the systems versus future feature and functionality requirements, which may include:
    1. Software infrastructure analysis reports
    2. Proactive software recommendation reports
    3. Software upgrade strategy reports
    4. Proactive critical bug analysis reports
    5. Software security alerts
h. Design Support: assist GSA in integrating technical requirements and design goals into the overall GSA network design while transferring design knowledge to the GSA team, which may include:
    1. Review of design requirements, priorities, and goals
    2. Analysis of impact of new requirements on the existing GSA network
    3. Review of network architecture and topology
    4. Review of protocol selection and configuration
    5. Review of feature selection and configuration
    6. Review of security considerations (i.e., authentication, VLANs, subnet isolation)
    7. Report describing the design with recommendations
    8. Provide ongoing incremental systems design and architectural consultation
    9. Provide ongoing information on design related systems security alerts that may impact key communications products.
i. Performance engineering and optimization: provide periodic performance analysis to sustain high performance systems and meet the changing demands on the GSA communications systems specific deliverables may include:
    1. Communications System's health assessments to include technology and/or routing protocols, including review of system devices health and collection of performance-related data
    2. Analysis of system's configurations against industry best practices
    3. Periodic SYSLOG analysis

4. Proactive advisory reports

j. Perform day to day maintenance and operations and provide Tier 3 support for the Unified Communications Infrastructure. While the infrastructure can and will evolve (and the contractor should provide recommendations to the Government as to what changes should be made), the team is currently delivering VoIP services to the vast majority of GSA employees through a Cisco Unified Communications Manager (CUCM) cluster distributed through four distinct hubs. This CUCM system routes calls to the Public Switched Telephone Network (PSTN) by SIP Trunking to Verizon (covered on a separate contract).

k. Design, develop, and maintain a number management system and processes to ensure the integrity of the GSA phone line inventory, to include periodic audits and cleanup of invalid numbers.

l. Provide for the collection and storage of Call Detail Records (CDRs) for ongoing IG investigations.

m. Execute knowledge of tools, processes and reporting towards proactive monitoring of voice quality statistics across the GSA Enterprise through unified communications endpoints

n. Maintain and improve voice quality standards through identification of and resolution of discovered issues

o. Provide support for GSA's Enterprise Fax solution to include support for SIP Trunking and call routing. This should also include evolving the system and recommending improvements for new solutions to provide fax service.

p. Provide support for GSA IT's Legacy Telecommunications services consists of analog, digital PSTN lines and trunks, as well as the management and maintenance of Private Branch Exchange (PBX) infrastructure including Contact Centers. Several FAS Contact Centers are supported using an Avaya based infrastructure. Additionally, GSA IT provides, through various contracts, audio conference bridges and calling cards.

q. Provide administrative level support for GSA IT's Web Conferencing Solution which is currently branded as "GSA Meeting Space". This support should include expertise on administering an Adobe Connect platform and making recommendations to GSA for improvements to the current system or evolving into a next generation Web Conferencing platform. Typical tasks include providing Tier 3 support to users and escalating tickets to our external Hosting or Audio Conferencing vendor, but the contractor needs to fully understand the product and be responsible for all day to day operations of the system, including recommending any future upgrades, modifications, or innovative alternative solutions.

r. Provide support for GSA IT's Enterprise Video Conferencing Solution, which is currently managed using Cisco Telepresence Management Suite. The system is made up exclusively of Cisco Telepresence products including Multipoint Control Units, Video Communications Servers, ISDN Gateways, Telepresence Content Servers, and Cisco endpoints. Additionally, GSA IT supports an Enterprise Video Streaming infrastructure, currently comprised of Helix Streaming servers, providing live event video streaming to the entire GSA enterprise network.

C.5.5.11 SUBTASK 11 - PROVIDE MOBILITY SUPPORT SERVICES

GSA requires full enterprise-wide architectural and operational support for its remote access infrastructure technologies, encompassing a virtualized desktop, application, and VPN solution. The existing environment consists of VMWare View, Citrix Xenapp, and Cisco VPN. GSA currently supports all three modes of remote access to allow GSA employees to telework. GSA is a leader in the Federal space on the use of telework, virtual employee environments and overall employee mobility to enhance employee productivity. The contractor shall provide shall operate and enhance the existing remote access offerings.

As part of mobility support services, the contractor shall:

a. Monitor, operate, maintain, and troubleshoot agency-wide, day-to-day Remote Access technologies to include, Virtualized Applications, Virtualized Desktop, and Virtual Private Networking. Current vendors are Citrix, VM Ware Horizon View, and Cisco, as well each of their supporting clients/plugins. central processing unit load, available disk space, along with remote access service availability must be tracked and alerts sent out to appropriate staff via email or other agreed upon escalation process when configured thresholds are exceeded. The contractor shall troubleshoot outages and service interruptions, conduct a root cause analysis, and prepare an Action Plan to prevent the outage in the future.
b. Provide Tier 3 subject matter expertise in Remote Access connectivity products/services (listed above), which includes, but is not limited to, system architecture, system administration, and system troubleshooting issues with Citrix Xenapp, Citrix Netscaler, Cisco Anyconnect client-based Secure Sockets Layer (SSL) VPN, and VMWare Horizon View Virtual Desktop Infrastructure (VDI) systems, end to end issues, from the backend server/appliance to the installed user client, including middleware supporting appliances. Current vendors are F5 (load balancing routers) and Cisco Whiptail storage.
c. Provide and maintain infrastructure documentation to include logical schematics and process flow of each remote access method in use. This documentation will be kept current at all times, and updated as situations warrant.
d. Assist in the engineering, planning, design, configuration, installation, maintenance, troubleshooting, monitoring, security, project management, documentation, testing, and support of GSA's Remote Access technologies.
e. Provide architecture optimizations/innovation options to help drive the future of remote access within GSA. It is expected for the contractor to regularly review the remote access industry 'landscape' and provide suggestions for refinements, new solutions, and technologies to help better enable GSA's desire for employee mobility.
f. Enable access to the GSA information infrastructure from anywhere at any time from any device.
g. Evaluate new technologies to provide faster and cost--effective networks to access information.

C.5.5.12 - SUBTASK 12 - PROVIDE CLIENT ENGINEERING SERVICE SUPPORT

GSA IT requires support for agency-wide client engineering services. The contractor shall provide management of the desktop/laptop operating systems including drivers and patches,

application, and configuration management. The contractor shall provide the client services listed below:

a. Automated software deployment support.
b. Image creation and compatibility.
c. Security Compliance to include patching, encryption, configuration management, energy management, remote device management, and reporting/visibility.

The contractor shall create the images that support GSA desktops/laptops that may connect directly to the GSA network and for the GSA IT VDI solution. The contractor shall provide Tier 3 support for all end-user (client) applications for desktops/laptops, and applications hosted in the VDI and Citrix environments. The contractor shall directly interface with, coordinate, and support the network, server services, and IT Security teams on issues that cross these functional areas while maintaining GSA Enterprise Architecture standards to ensure a consistent and compatible configuration for GSA client infrastructure.

In support of client engineering services, the contractor shall:

a. Provide Tier 3 technical support services across the GSA enterprise for agency-wide end-user computing platforms for desktops, laptops, and mobile devices; device configuration; technical refresh and customer data migration from one machine to another; and service activities processed in a seamless manner (cradle-to-grave) with a single point of contact with the customer for all activities.
b. Provide comprehensive support for GSA client applications on agency-provided hardware while providing best-effort support for user-owned devices. Client Engineering provides Tier 3 support for enterprise applications.
c. Provide automated software deployment to GSA user workstations via a standardized enterprise management solution.
d. Take corrective actions to maintain service and quality levels.
e. Develop and maintain GPOs to enforce consistency in GSA IT's deployed client hardware inventory.
f. Support testing of new hardware and software for possible deployment in the environment.
g. Create the quarterly "Gold" image that will be used on GSA's physical client hardware and as the basis for the GSA VDI image. Although GSA attempts to maintain a single "Gold" image we may require support for multiple images for new Operating System versions, VDI requirements, and special needs. We require a quarterly update on the Gold image and monthly on the VDI image.
h. Develop software delivery packages for the removal, replacement, and/or upgrading of applications and patches required on 10 or more workstations up to the enterprise level (all workstations). It is incumbent upon the contractor to support all software on GSA laptops and desktops and assist in the deployment, maintenance, and clean-up whether by retirement and or removal of software that does not have a migration path towards the EA approved list (Section J, Attachment V, Attachment 6).
i. Provide effective management of all software loaded on GSA client hardware.

j. Provide Tier 3 support of other GSA teams on any issues that involves end-user hardware or/software.

C.5.6 TASK 6 – PROVIDE ENTERPRISE IT INFRASTRUCTURE AS-NEEDED CAPABILITIES - SURGE.

The contractor shall support planned and unplanned surge support services. These support services may cross all task and subtask areas within the TO. The contractor shall account for surge activities and provide the resources necessary to accommodate them without burdening Government and contractor operational staff. During the life of the TO, the workload in any one area may grow significantly for a period of time. Some activities are recurring while others are not. Recurring activities include, but are not limited to, audit support, the annual physical inventory of IT assets, year-end procurements, and technology refresh cycles. Examples of non-recurring activities include major system rollouts, major office moves, presidential transition activities, COOP/DR events, unexpected increases in Federal staffing to meet GSA mandates, infrastructure initiatives to meet external regulatory mandates, and implementation of new GSA programs and projects.

For project support work, the contractor shall develop project and design plans, and once the plans and scheduled dates are mutually agreed to between the Government and contractor, the contractor shall ensure actual implementation dates do not deviate from the planned schedule dates by more than 14 calendar days.

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

D.1 PRESERVATION, PACKAGING, PACKING, AND MARKING

All deliverables submitted to the Government shall indicate the contract number, TO number, contractor's name, description of items contain therein and the consignee's name and address for which the information is being submitted. The contractor shall follow the marking requirements specified by the Government.

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

E.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates the following clauses by reference with the same force and effect as if they were given in full text. Upon request, the CO will make their full text available. Also, the full text of a provision may be accessed electronically at:

FAR website: https://www.acquisition.gov/far/

CLAUSE #	CLAUSE TITLE	DATE
52.246-5	Inspection of Services – Cost Reimbursement	(Apr 1984)

E.2 PLACE OF INSPECTION AND ACCEPTANCE

The inspection and acceptance of all work performance, reports, and other deliverables under this TO shall be performed by the COR and the TPOC.

E.3 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the COR and the TPOC. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.4 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the TO, the contractor's proposal, and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

For IT development, the final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables must either be incorporated in the succeeding version of the deliverable, or the contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the requirements stated within this TO, the document may be immediately rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the COR.

E.5 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in Section F) from Government receipt of the draft deliverable. Upon receipt of the Government's comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

E.6 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The CO/COR will provide written notification of acceptance or rejection (Section J, Attachment J) of all final deliverables within 15 workdays (unless specified otherwise in Section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.7 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the award fee determination report, and there will be an associated reduction in the earned award fee.

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

F.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates the following clauses by reference with the same force and effect as if they were given in full text. Upon request the CO will make their full text available. Also, the full text of a provision may be accessed electronically at:

FAR website: https://www.acquisition.gov/far/

CLAUSE #	CLAUSE TITLE	DATE
52.242-15	Stop-work Order	(Aug 1989)
52.242-15	Stop-work Order (Alternate I)	(Apr 1984)

F.3 TASK ORDER PERIOD OF PERFORMANCE

The period of performance for this TO is a 12-month base period and four 12-month option periods as follows:

a. Base Period: October 13, 2015 – October 12, 2016
b. Option Period 1: October 13, 2016 – October 12, 2017
c. Option Period 2: October 13, 2017 – October 12, 2018
d. Option Period 3: October 13, 2018 – October 12, 2019
e. Option Period 4: October 13, 2019 – October 12, 2020

F.4 PLACE OF PERFORMANCE

The primary place of performance is contractor facilities unless otherwise specified. GSA CONUS and OCONUS locations are identified in Section J, Attachment L. The contractor may be required to travel to any of the GSA locations in support of the task order.

F.5 DELIVERABLES

The following schedule of milestones will be used by the COR and TPOC to monitor timely progress under this TO.

The following abbreviations are used in this schedule:

IAW: In Accordance With
NLT: No Later Than
PS: Project Start
TOA: Task Order Award
WD: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

The contractor shall submit the deliverables listed in the following table:

MILESTONE/DELIVERABLE	CLIN	TOR REFERENCE	PLANNED COMPLETION DATE	DATA RIGHTS CLAUSE
Project Start (PS)			NOV 04, 2015	
Kick-Off Meeting	X001	C.5.1.1	PS	52.227-14
Copy of TO (initial award and all modifications)		F.5.1 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT	Within 10 WD of PS (initial award and all modifications)	52.227-14
Monthly Status Report	X001	C.5.1.2	Monthly, 10th calendar day of the next month (EVM and Financials, Para C.5.1.2.g –i due by the 15th calendar day)	52.227-14
Transition-In Plan – Draft	X001	C.5.1.12	Due at Kick-Off Meeting	52.227-14
Transition-In Plan – Comments	X001	C.5.1.12	15 WD after Government receipt	52.227-14
Transition-In Plan – Final	X001	C.5.1.12	10 WD after receipt of Government comments	52.227-14
Project Management Plan	X001	C.5.1.5, C.5.1.6, C.5.1.8, C.5.1.13	Due at Kick-Off Meeting, updated every six months	52.227-14
Project Management Plan – Comments	X001	C.5.1.5, C.5.1.6, C.5.1.8, C.5.1.13	15 WD after Government receipt	52.227-14
Project Management Plan – Final	X001	C.5.1.5, C.5.1.6, C.5.1.8, C.5.1.13	10 WD after receipt of Government comments	52.227-14
Technical Status Meeting - Agenda and Minutes	X001	C.5.1.4	Monthly – Agenda two WD prior and Minutes two WD post meeting	52.227-14
Weekly Operational Meeting - Agenda and Minutes	X001	C.5.1.4	Weekly - Agenda two WD prior and Minutes two WD post meeting	52.227-14
Trip Report(s)	X001	C.5.1.7	Within 10 WD following completion of each trip	52.227-14
Transition-Out Plan	X001	C.5.1.12	Annually - 90 calendar days from the expiration of TO period of performance	52.227-14

MILESTONE/DELIVERABLE	CLIN	TOR REFERENCE	PLANNED COMPLETION DATE	DATA RIGHTS CLAUSE
Transition-Out Plan – Final	X001	C.5.1.12	10 WD after receipt of Government comments	52.227-14
*CSI Register	X001	C.5.1.13	PS + 4 Months - updated weekly	52.227-14
Section 508 Product Accessibility Report	X001		NLT 20 WD after PS and upon system changes affecting the report	52.227-14
IT Security Plan	X001	F.5.2 GSA Information Technology (IT) Security Requirements	Nov 27, 2015 and annual update	52.227-17
IT Security Authorization	X001	F.5.2 GSA Information Technology (IT) Security Requirements	PS + 6 months	52.227-17
IT Service Management Plan	X002	C.5.2.1	PS + 3 Months – updated annually	52.227-14
*Demand Management Report	X002	C.5.2.4	PS + 4 Months - updated weekly	52.227-14
IT Optimization and Transformation Plan	X002	C.5.3.1	PS + 6 Months – updated annually	52.227-14
Emerging Technology and Innovation Plan	X002	C.5.3.1	04MAY2016 – updated as required	52.227-14
Emerging Technology and Innovation Reports	X002	C.5.3.1	04AUG2016 – updated every six months or as requested	52.227-14
As-Is and To-Be Infrastructure Architectures	X002	C.5.3.2	Draft 13MAY2016, Final 30JUN2016 – updated annually	52.227-14
Capacity Management Plan	X002	C.5.3.3	PS + 6 Months – updated every six months	52.227-14
*Capacity Management Reports	X002	C.5.3.3	PS + 4 Months – updated weekly	52.227-14
Availability Management Plan	X002	C.5.3.4	11MAR2016 – update 30SEPT2016 then every six months	52.227-14
*Availability Management Reports	X002	C.5.3.4	PS + 4 Months – updated weekly	52.227-14
Service Quality Plan	X002	C.5.3.6	PS + 4 Months – updated every six months	52.227-14

MILESTONE/DELIVERABLE	CLIN	TOR REFERENCE	PLANNED COMPLETION DATE	DATA RIGHTS CLAUSE
Service Level Requirements	X002	C.5.3.6	11MAR2016 – reviewed and updated every six months or as requested	52.227-14
Service Level Management Plan	X002	C.5.3.6	15APR2016, updated 15SEP2016 then every six months	52.227-14
Service Level Agreements	X002	C.5.3.6	PS + 4 Months – reviewed and updated every six months or as requested	52.227-14
Service Improvement Plan	X002	C.5.3.6	11MAR2016 – reviewed and updated every six months or as requested	52.227-14
Operational Level Agreements	X002	C.5.3.6	Within 60 Calendar Days of PS	52.227-14
*Service Catalogue	X002	C.5.2.3, C.5.3.7	PS + 4 Months, updated daily	52.227-14
Enterprise IT Services Dashboard Plan	X002	C.5.3.8	PS + 90 WD	52.227-14
Enterprise IT Services Dashboard	X002	C.5.3.8	PS + 6 Months	52.227-17
COOP Plan	X002	C.5.3.9	11MAR2016 – update 31AUG2016 then every six months"	52.227-14
Contingency Plans	X002	C.5.3.9		
EAS Information System Contingency Plan	X002	C.5.3.9	11MAR2016 – update 29JUL2016 then review and update as required every six months	52.227-14
EMD Information System Contingency Plan	X002	C.5.3.9	11MAR2016 – update 31MAY2016then review and update as required every six months	52.227-14
ENS Information System Contingency Plan	X002	C.5.3.9	11MAR2016 – update 30JUN2016 then review and update as required every six months	52.227-14
EMD-NSD Information System Contingency Plan	X002	C.5.3.9	11MAR2016	52.227-14

MILESTONE/DELIVERABLE	CLIN	TOR REFERENCE	PLANNED COMPLETION DATE	DATA RIGHTS CLAUSE
ESS Information System Contingency Plan	X002	C.5.3.9	11MAR2016 – update 29APR2016 then review and update as required every six months	52.227-14
IT Playbook Plan	X002	C.5.3.9	11MAR2016 – update 31AUG2016 then every six months or as required	52.227-14
IT Service Continuity Management Plan	X002	C.5.3.9	11MAR2016 – update 31AUG2016 then every six months or as required	52.227-14
Test Plans	X002	C.5.4.4	As needed	52.227-14
Release and Deployment Management Plan	X002	C.5.4.3	11MAR2016 – update 30SEPT2016 then every six months	52.227-14
SACM Management Plan	X002	C.5.4.5	04MAR2016 – updated 16SEPT2016 then every six months	52.227-14
Equipment Spares Inventory Management Plan	X002	C.5.4.5	04MAR2016 – updated 16SEPT2016 then every six months	52.227-14
*Knowledge Base	X002	C.5.5.1, C.5.4.1	PS + 4 Months - updated daily	52.227-14
*Incident Reports	X002	C.5.5.1	Within 4 hours of incident identification	52.227-14
*Root Cause Analysis reports	X002	C.5.5.1	Within 3 WD of incident/ problem resolution	52.227-14
Network Performance Plan	X002	C.5.5.8	11MAR2016 – update 11NOV2016 then every six months"	52.227-14
*Network Performance Analysis Reports	X002	C.5.5.8	PS + 4 months, updated weekly	52.227-14
Network Capacity Plan	X002	C.5.5.8	11MAR2016 – update 11NOV2016 then every six months"	52.227-14
*Network Capacity Analysis Reports	X002	C.5.5.8	PS + 4 months, updated monthly	52.227-14
Network Modernization Plan	X002	C.5.5.8	30JUN2016 – updated annually	52.227-14
EIOC Transformation Plan	X002	C.5.5.9	PS + 6 Months, updated annually	52.227-14

MILESTONE/DELIVERABLE	CLIN	TOR REFERENCE	PLANNED COMPLETION DATE	DATA RIGHTS CLAUSE
EIOC Escalation Procedures	X002	C.5.5.9	60 WD after PS – updated 03MAY2016 then every six months or as required	52.227-14
Project and Design Plans	X003	C.5.6	As needed	52.227-14
Contractor Access List Security Report	X001	H.7.1.3	25th of every Month	52.227-14
Small Business Utilization report	X001	H.28	PS + 6 months, updated every six months	52.227-14
Ad Hoc Reports	X001-X003		Ad Hoc	52.227-14

*These deliverables/reports are anticipated to be required as stated in the table, however, the frequency or need for the report may be adjusted over time, or replaced by the Enterprise IT Services Dashboard automated reporting in Section C.5.3.8.

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-confirming markings in accordance with subparagraphs (e) and (f) of the FAR clause at 52.227-14.

F.5.1 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA. The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall demonstrate why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider all of the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.5.2 GSA INFORMATION TECHNOLOGY (IT) SECURITY REQUIREMENTS

The contractor shall deliver an IT Security Plan on or before Nov 27, 2015 that describes the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this order. The IT Security Plan shall comply with applicable Federal laws including, but are not limited to, 40 U.S.C. 11331, the FISMA of 2002, and the E-Government Act of 2002. The IT Security Plan shall meet IT security requirements in accordance with Federal and GSA policies and procedures, including GSAR clause 552.239-71. The contractor shall submit written proof of IT security authorization six months after award, and verify that the IT Security Plan remains valid annually.

F.5.3 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by email and removable electronic media, as well as placing in the GSA IT and FEDSIM designated repository. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

- Text: MS Word or Google equivalent
- Spreadsheets: MS Excel or Google equivalent
- Briefings: MS PowerPoint or Google equivalent
- Drawings: MS Visio
- Schedules: MS Project or Smartsheet

F.6 PLACE(S) OF DELIVERY

Unclassified deliverables and correspondence shall be delivered to the GSA CO or COR at the following address:

GSA FAS AAS FEDSIM
ATTN: Mr. Derrick White, CO
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405
Telephone: (571) 814-0184
Email: derrick.white@gsa.gov

GSA FAS AAS FEDSIM
ATTN: Mr. Domnic Salli, COR
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405
Telephone: (202) 208-7931
Email: dominic.salli@gsa.gov

Copies of all deliverables shall also be delivered to the GSA IT TPOC.

ATTN: Ms. Debra Anne
1800 F Street NW

Washington, D.C. 20405
Telephone: (202) 694-2951
Email: debra.anne@gsa.gov

F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the COR via a Problem Notification Report (PNR) (Section J, Attachment I) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

G.3.5 CONTRACTING OFFICER'S REPRESENTATIVE

The CO will appoint a COR in writing through a COR Appointment Letter that will be provided to the contractor upon award (Section J, Attachment A). The COR will receive, for the Government, all work called for by the TO and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to contractor personnel.

The COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by a CO through a properly executed modifications to the Contract or the TO.

G.3.5.1 CONTRACT ADMINISTRATION

Contracting Officer:

Derrick White
GSA FAS AAS FEDSIM
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405
Telephone: (571) 814-0184
Email: derrick.white@gsa.gov

Contracting Officer's Representative:

GSA FAS AAS FEDSIM
ATTN: Mr. Dominic Salli, COR
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405
Telephone: (202) 208-7931
Email: dominic.salli@gsa.gov

Technical Point of Contact:

Ms. Debra Anne
1800 F Street NW
Washington, D.C. 20405
Telephone: (202) 694-2951
Email: debra.anne@gsa.gov

G.9.6 INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice.

Task Order Number: GSQ0015AJ0022
Paying Number: (ACT/DAC NO.) (From GSA Form 300, Block 4)
FEDSIM Project Number: 15010GSM
Project Title: GSA Enterprise Operations (GEO)

The contractor shall certify with a signed and dated statement that the invoice is correct and proper for payment.

The contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category.

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Assisted Services Shared Information SysTem (ASSIST) to submit invoices. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Log in using your assigned ID and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the *Create New Invoice* button. The Assisted Acquisition Service Business Systems (AASBS) Help Desk should be contacted for support at 877-472-4877 (toll free) or by email at AASBS.helpdesk@gsa.gov. By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. However, the FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment.

G.9.6.1 INVOICE REQUIREMENTS

The contractor shall submit an advance copy of an invoice to the COR and TPOC for review prior to its submission to GSA. Receipts are provided on an as requested basis.

If the TO has different contract types, each should be addressed separately in the invoice submission.

The final invoice is desired to be submitted within six months of project completion.

G.9.6.1.1 COST-PLUS-AWARD-FEE (CPAF) CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), **Task and Sub Task**, by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name
b. Employee Alliant labor category
c. Monthly and total cumulative hours worked

d. Corresponding TO bid rate
e. Employee billing rate
f. Cost incurred not billed
g. Current approved forward pricing rate agreement in support of indirect costs billed
h. The contractor shall identify charges for internal and external clients according to use (i.e. a functioning equitable and transparent service charge back mechanism and model in place across the enterprise) as detailed in Section C.5.2.2.

All cost presentations provided by the contractor shall also include Overhead charges and General and Administrative charges and shall also include the Overhead and General and Administrative rates being applied.

The Government will promptly make payment of any award fee upon the submission, by the contractor to the COR, of a public voucher or invoice in the amount of the total fee earned for the period evaluated. Payment may be made without issuing a TO modification if funds have been obligated for the award fee amount. The contractor shall attach the Award Fee Determining Official determination letter to the public voucher and/or invoice.

G.9.6.1.2 OTHER DIRECT COSTS (ODCs)

The contractor may invoice monthly on the basis of cost incurred for the ODC CLIN. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

a. Tools and/or ODCs purchased
b. Consent to Purchase number or identifier
c. Date accepted by the Government
d. Associated CLIN
e. Project-to-date totals by CLIN
f. Cost incurred not billed
g. Remaining balance of the CLIN

All cost presentations provided by the contractor shall also include Overhead charges, General and Administrative charges, and Fee in accordance with it's DCAA cost disclosure statement.

G.9.6.1.3 TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Joint Travel Regulation (JTR) - prescribed by the GSA, for travel in the contiguous U.S.

b. FTR Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.

Local travel will not be reimbursed in performance of this TO.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR/FTR. Long distance travel is defined as travel over 50 miles from the employee

place of employment. The invoice shall include the period of performance covered by the invoice, the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN/Task Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN/Task. The current invoice period's travel details shall include separate columns and totals and include the following:

a. Travel Authorization Request number or identifier, approver name, and approval date
b. Current invoice period
c. Names of persons traveling
d. Number of travel days
e. Dates of travel
f. Number of days per diem charged
g. Per diem rate used
h. Total per diem charged
i. Transportation costs
j. Total charges
k. Explanation of variances exceeding 10% of the approved versus actual costs
l. Indirect Handling Rate

All cost presentations provided by the contractor shall also include Overhead charges and General and Administrative charges IAW it's DCAA approved practices.

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

H.2 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform this TO. The contractor may augment its "Key" team with up to four additional Key Personnel as appropriate to its solution.

a. Program Manager (PM)
b. Service Delivery Manager
c. Service Desk Manager
d. Infrastructure Operations Manager
e. IT Infrastructure Architect
f. Chief Technologist
g. Data Center Migration Manager
h. Transition Manager
i. Security Manager

The Key Personnel specified in the contractor's proposal shall be available on TO award. The Government desires that Key Personnel be assigned for the duration of the TO.

All Key Personnel must possess excellent oral and written communication skills, be fluent in English, and possess experience in presenting material to senior Government officials.

Below is the Key Personnel Table referencing Key Personnel by position and name.

Key Personnel Table

Position	Name
Program Manager (PM)	(b) (6)
Service Delivery Manager	
Service Desk Manager	
Infrastructure Operations Manager	
IT Infrastructure Architect	
Chief Technologist	
Data Center Migration Manager	
Transition Manager	
Security Manager	

H.2.1 PROGRAM MANAGER (PM)

The contractor shall identify a full-time, single PM to serve as the Government's primary POC and to provide overall leadership and guidance for all contractor personnel assigned to the TO. The PM is ultimately responsible for the quality and efficiency of the TO, to include both technical issues and business processes. The PM shall be an employee of the prime

contractor. This PM shall have the authority to commit the contractor's organization and make decisions for the contractor's organization in response to Government issues, concerns, or problems. This person shall be readily available to respond to Government questions, concerns, and comments, as well as be proactive in alerting the Government to potential contractual or programmatic issues including situations that may comprise the contractor's ability to provide services.

It is required that the PM has the following qualifications:

a. Certified Project Management Professional Certification (Project Management Professional or Program Management Professional (PgMP)) at the time of proposal Part III submission.
b. ITIL® Foundation Level Certification (or better) at the time of proposal Part III submission.

It is desirable that the PM has the following qualifications:

a. A minimum of 10 years of experience with the management of an Enterprise IT Service Delivery and Management Program similar in size, scope, and complexity to the requirements of this Task Order Request (TOR).
b. Experience with the management, manpower utilization, and supervision of employees (including subcontractors) of various labor categories and skills in projects similar in size and scope as proposed for this TOR.
c. Experience leading the successful transition of IT service delivery to an ITIL/ITSM framework for a large, worldwide organization.
d. Familiarity with the Federal procurement process.
e. Familiarity with the administration of cost-type contracts.

H.2.2 SERVICE DELIVERY MANAGER

The Service Delivery Manager shall manage all service delivery-related processes and the delivery of projects from engineering to operation; shall be the service owner for all end user and customer-facing IT services and solutions; and shall ensure end-to-end delivery of services based on Government-approved ITSM processes consistent with industry best practices.

It is required that the Service Delivery Manager has the following qualifications:

a. Certified Project Management Professional Certification (Project Management Professional or PgMP) at the time of proposal Part III submission.
b. ITIL® Expert Level Certification (or better) at the time of proposal Part III submission.
c. Experience in providing Enterprise IT Services similar in size, scope, and complexity to the requirements of this TOR, including implementation of ITIL best practices.

It is desirable that the Service Delivery Manager has the following qualifications:

a. Demonstrated success improving, optimizing, standardizing, and streamlining customer support processes that yielded improvements in customer satisfaction and resulted in cost reductions.
b. Five years' experience managing IT service delivery requirements similar in size, scope and complexity to this TOR.

c. Five years' experience managing service desk teams supporting the requirement similar in size, scope, and complexity to this TOR.Demonstrated experience providing performance-based customer service support against multiple performance metrics in the Federal Government.
d. Experience in communicating with Government personnel, including agency executives.

H.2.3 SERVICE DESK MANAGER

The Service Desk Manager shall manage the performance of service desk and deskside services to users. The Service Desk Manager will provide users efficient and timely first and second level support to ensure that service levels are achieved in line with the TO and that customer expectations are met or exceeded. The Service Desk Manager shall be located at the contractor's service desk facility.

It is required that the Service Desk Manager has the following qualifications:

a. Certified ITIL® Intermediate Level Certification (or better) in at least one Service Capability or Service Lifecycle Module at time of proposal Part III submission.
b. Certified Project Management Professional Certification (Project Management Professional or PgMP)) at time of proposal Part III submission.
c. Five or more years of related technical and managerial experience in an end-to-end service desk and deskside service delivery environment similar in terms of size, scope and complexity to that of this TOR.

It is desirable that the Service Desk Manager has the following qualifications:

a. Help Desk Institute or Service Desk Institute Service Desk Manager Certification.
b. Certified ITIL® Intermediate Level Certification (or better) in two or more Service Capability or Service Lifecycle Modules at time of proposal Part III submission.
c. Demonstrated success improving, optimizing, standardizing, and streamlining customer support processes that yielded improvements in customer satisfaction and resulted in cost reductions.
d. Demonstrated experience and proven success implementing changes, processes, and standards to improve an enterprise-wide service desk.
e. Demonstrated experience with service desk technologies proposed by the contractor.
f. Demonstrated experience providing performance-based customer service support against multiple performance metrics in the Federal Government.
g. Demonstrated in-depth experience with the implementation and customization of service desk tools and automation technologies.

H.2.4 INFRASTRUCTURE OPERATIONS MANAGER

The Infrastructure Operations Manager shall manage all operations-related processes, ensures the operation of the Enterprise meets defined service levels, and serves as the contractor's service owner for all IT services and solutions.

It is required that the Infrastructure Operations Manager has the following qualifications:

a. Certified ITIL® Intermediate Level Certification (or better) in at least one Service Capability or Service Lifecycle Module at time of proposal Part III submission.
b. Certified Project Management Professional Certification (Project Management Professional or PgMP) at time of proposal Part III submission.
c. Experience managing IT Infrastructure Engineering and Operations similar to this TO and the contractor's proposed solution to include Data Centers, Cloud provided IT solutions, WAN/LAN, and Server Support.

It is desired that the Infrastructure Operations Manager has the following qualifications:

a. Active CISCO Certified CISCO Internetwork Expert (CCIE) Certification at the time of proposal Part III submission.
b. Certified ITIL® Intermediate Level Certification (or better) in two or more Service Capability or Service Lifecycle Modules at time of proposal Part III submission.
c. Demonstrated experience operating and designing a network supporting a dispersed workforce with on-premise applications as well as many applications deployed in the cloud.
d. Two or more years of experience managing a Network Operations Center of representative size and complexity as that of this TOR.
e. Demonstrated experience with IT infrastructure technologies including but not limited to Windows and Linux operating systems and associated technologies, storage systems, local and wide area network infrastructure, server hardware, video and voice systems, remote access solutions, messaging, mobility, monitoring tools, TCP/IP and DNS and other foundational protocols, Active Directory, and virtualization platforms. Knowledge and experience with client server, cloud computing (private, public, and hybrid) and enterprise collaboration technologies.
f. Demonstrated expert experience with troubleshooting a wide range of LAN, MPLS WAN, Wi-Fi and SAN, network issues hampering service availability and making recommendations for system fixes and enhancements.
g. Demonstrated experience with WAN Optimization appliances and with sophisticated tools for capacity planning and predicative analytics for bandwidth trending
h. Demonstrated experience with leveraging tools to manage router and switch configurations. In addition, experience with using tools to manage all critical router and switch functions.
i. Five or more years of management experience operating in an ITIL framework.

H.2.5 IT INFRASTRUCTURE ARCHITECT

The IT Infrastructure Architect shall provide technical expertise to translate business requirements into value added services and cost efficient IT Infrastructure solutions across multiple technologies and ensure continuous transformation of GSA's IT Infrastructure to meet the evolving demands of the GSA systems and workforce.

It is required that the IT Infrastructure Architect has the following qualifications:

a. Experience planning, designing, and upgrading complex IT infrastructure environments similar in size and scope as referenced in this TOR.

It is desired that the IT Infrastructure Architect has the following qualifications:

a. Active CISCO Certified CISCO Internetwork Expert (CCIE) or CISCO Design Expert (CCDE) Certification(s) at the time of proposal Part III submission.
b. Certified ITIL® Intermediate Level Certification (or better) in at least one Service Capability or Service Lifecycle Module at time of proposal Part III submission.
c. Demonstrated experience working collaboratively with customer stakeholders to enhance and modernize IT infrastructure to align with client business portfolios and service-level requirements.
d. Demonstrated experience managing complex IT infrastructure and developing scalable enterprise technology strategies across multiple platforms.
e. Demonstrated experience with IT infrastructure technologies including but not limited to Windows and Linux operating systems and associated technologies, storage systems, local and wide area network infrastructure, server hardware, video and voice systems, remote access solutions, messaging, mobility, monitoring tools, TCP/IP and DNS and other foundational protocols, Active Directory, and virtualization platforms. Knowledge and experience with client server, cloud computing (private, public, and hybrid) and enterprise collaboration technologies.
f. Demonstrated experience making recommendations for leveraging network installations and reducing operation costs.
g. Demonstrated experience operating and designing a network using routing protocols BGP, OSPF, EIGRP, Layer-3/-2 MPLS VPN, IPsec VPN. Understands BGP route reflectors, BGP peering and BGP regular expressions.

H.2.6 CHIEF TECHNOLOGIST

The Chief Technologist shall provide technology vision and leadership in the development and implementation of services for this TO. This individual shall lead the contractor in planning and implementing enterprise information systems to support both distributed and centralized business operations and achieve more effective and cost-beneficial, enterprise-wide IT operations. The Chief Technologist shall lead the translation and estimation of business system IT needs into support requirements, including impact on current support operations and capabilities, risk analysis of proposed migrations, and supportability of new technologies.

It is required that the Chief Technologist has the following qualifications:

a. Experience as a Chief Technology Officer (CTO), Chief Information Officer (CIO) or Organizational-Wide Enterprise Architect.
b. Experience designing, engineering, implementing, and operating enterprise infrastructures similar to what is needed for the GEO IT environment.

It is desired that the Chief Technologist has the following qualifications:

a. ITIL® Expert Level Certification at time of proposal Part III submission
b. Demonstrated success in major technology innovation engagements for enterprise clients.
c. Five years' experience as a CTO, CIO or Organizational-Wide Enterprise Architect.
d. 10 years of experience in IT Service Delivery Management.
e. Three or more years of direct management of a major IT operation.

f. Experience translating organizational business and architectural needs into requirements, logical and physical designs, and service deployments.

Experience with the successful integration of a wide range of original equipment manufacturer and technology leaders.

H.2.7 DATA CENTER MIGRATION MANAGER (DCM)

Data Center Migration planning and coordination is a key activity that shall be led by the IT Infrastructure Architect with the dedicated support of a Data Center Migration Manager SME. DCM provides cross-organization guidance and supervision for data center consolidations.

It is required that the Data Center Migration Manager has the following qualifications:

a. Possesses up to Top Secret clearance level
b. Certified ITIL® Intermediate Level Certification (or better) in at least one Service Capability or Service Lifecycle Module
c. 15 years of IT experience; 9 years of specialized experience managing IT Infrastructure Engineering and Operations and 7 years' of experience managing CPAF contracts

It is desired that the Data Center Migration Manager has the following qualifications:

a. Experience with the management, manpower utilization, and supervision of employees (including subcontractors) of various labor categories and skills.
b. Experience leading the successful transition of IT infrastructure into an enterprise class data center.
c. Experience evaluating data center environment for its ability to support IT service requirements. (e.g., power, battery backup, generator, HVAC, etc.).
d. Excellent oral and written communication skills, be fluent in English, and possess experience in presenting material to senior Government officials.

H.2.8 TRANSITION MANAGER

The Transition Manager shall be responsible for the seamless execution of the Transition-In Plan.

It is required that the Transition Manager have the following qualification:

a. Experience in planning and executing Federal Government contract transitions similar in size, scope, and complexity to the requirements of this Task Order Request (TOR).

It is desired that the Transition Manager has the following qualifications:

a. Experience in identifying and hiring incumbent staff from the departing contractor(s) to the new prime contractor.

b. Experience in successfully leading and managing project teams, including the use of project scheduling, monitoring, and reporting tools; resource management; and effective collaboration techniques.
c. Excellent oral and written communication skills and possess experience in presenting transition plans and status to senior management and Government officials.

H.2.9 SECURITY MANAGER

The Security Manager shall manage all coordination amongst security tasks and providers. Shall harmonize processes to "bake in" security features from the beginning rather than "bolt on" at the end.

It is required that the Security Manager has the following qualifications:

a. Demonstrated IT experience with specialized experience in Cybersecurity
b. Possesses up to Top Secret clearance level
c. Active CISSP certification.

It is desired that the Security Manager has the following qualifications:

a. Certified Project Management Professional Certification (Project Management Professional or Program Management Professional (PgMP))
b. Five years experience implementing NIST 800-53 security controls and documenting System Security Plans for IT infrastructure similar to the requirements of this Task Order Request (TOR).
c. Five years experience developing and documenting processes to comply with NIST 800-53 security controls.
d. Three years experience with FISMA reporting.
e. Demonstrated experience implementing risk-based security programs.
f. Two years experience creating, reviewing, and analyzing Interconnection Security Agreements and supporting Memorandum of Agreement/Understanding (MOA/U).
g. Three years experience recommending security architecture and security monitoring improvements.
h. Familiarity with automating security-related tasks to support continuous monitoring.
i. Excellent oral and written communication skills and possess experience in presenting transition plans and status to senior management and Government officials.

H.2.10 NON-KEY PERSONNEL REQUIREMENTS

All personnel assigned to the TO and who have access to the GSA systems must meet the necessary security standards required before they can be given badges or passwords (see H.7). It is desired that all personnel assigned shall, within 12 months of being assigned, have ITIL® Intermediate Level Certification. In addition, it is desired that the non-key Project Managers have an active certification in accordance with Project Management Institute (PMI) Project Management Body of Knowledge (PMBOK) as a Project Management Professional.

H.2.11 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the CO. Prior to utilizing other than personnel specified in proposals in response to a TOR, the contractor shall notify the Government CO and the COR of the existing TO. This notification shall be no later than five calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute personnel qualifications shall be equal to, or greater than, those of the personnel being substituted. If the Government CO and the COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6, Termination (Cost Reimbursement). All substitute personnel must be oriented and trained for TO performance at the contractor's expense.

H.2.12 CONTRACTOR PERSONNEL REMOVAL AND REPLACEMENT

The Government CO and COR may require the contractor to remove and/or replace contractor personnel during the life of the TO.

Contractor personnel may be removed and/or replaced should it be determined that the individual(s) is a potential threat to the health, safety, security, general well-being or operational mission of the agency and its facilities, systems, and/or population.

H.5 GOVERNMENT-FURNISHED PROPERTY (GFP)

GFP provided will change throughout the life of the TO. Initially, the Government envisions furnishing the contractor with the following equipment:

a. Work space as necessary with at least touchdown space with one laptop with softphone application (currently Cisco IP Communicator) for individuals assigned full time to a GSA facility. In addition, onsite performance will include containers for document storage and access to network multifunction printers.
b. Laptop computers and mobile devices (smart phones) as needed.
c. Passwords and access cards and/or tokens (upon completion of security requirements) to systems and devices required for performance of the work.
d. For contractor personnel not located in Government space, GSA will provide remote access to the GSA network.
e. The Government will provide the EITM system, a GSA IT Service Desk email account, and Service Desk toll-free numbers.
f. The Government will initially furnish network monitoring and diagnostic tools as GFP.

H.5.2 GOVERNMENT-FURNISHED INFORMATION (GFI)

The Government will furnish the contractor with the documentation available for existing hardware and software in use as part of GSA's operations (such as the EITM system). In addition, detailed descriptions of GSA's current IT platforms, customers, locations, and other technical information needed to perform the TO will be provided during the Transition-In period.

The contractor will have access to the GSA network and all information, resources, and data that comes with GSA IT access.

H.7 SECURITY CONSIDERATIONS

Contractors entering into an agreement for IT services and products with GSA and/or its Federal customers shall be contractually subject to all GSA and Federal IT Security standards, policies, and reporting requirements. GSA must provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

The contractor shall comply with GSA Order 2100.1 – IT Security Policy, GSA Order ADM 9732.1D – Suitability and Personnel Security Chapter 6, and GSA Order

Chief Information Officer (CIO) P 2181 –HSPD-12 Personal Identity Verification and Credentialing Handbook and adhere to all security-related laws, requirements, and regulations that bind the Government.

The contractor shall insert the TO security considerations in all subcontracts when the subcontractor is required to have physical access to a federally controlled facility or access to a Federal information system.

Termination of any employee with access to GSA IT systems shall be reported to GSA within 60 minutes. The contractor is responsible for revoking all access to GSA systems within 60 minutes of employee (prime or sub-contractor) termination.

H.7.1 HSPD-12 AND SECURITY AND PRIVACY AWARENESS TRAINING

H.7.1.1 HSPD-12 PERSONNEL IDENTITY VERIFICATION

The contractor shall comply with agency personal identity verification procedures identified in the TOR that implement HSPD-12 Information Processing Standards Publication (FIPS PUB) Number 201. All contractor personnel who require access to GSA information systems, including contractor operations that design, operate, test, maintain, and/or monitor GSA systems, shall be subject to background investigations and must receive a favorable background investigation from GSA.

Contractor administrative/clerical personnel performing on this TO have been determined to meet the security criteria for and are designated as “Low Risk” positions. In accordance with established security procedures, contractors working in positions designated Low Risk must have a National Agency Check and Inquiries (NACI).

Contractor personnel, other than contractor administrative/clerical personnel, performing on this contract have been determined to meet the security criteria for and are designated as “Moderate Risk” positions and must have a Minimum Background Investigation.

The contractor shall coordinate all requests for investigations with the COR and TPOC or other designated Government POC to ensure that each request meets the criteria for determining the position sensitivity risk designation.

The contractor, when notified of an unfavorably adjudicated background investigation on a contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.

The contractor shall be responsible for managing its workforce to ensure that sufficient contract personnel who meet all suitability requirements are available to perform the duties required under this TO. New or replacement contract personnel must have previously received a favorable suitability determination in sufficient time to perform work on-site at GSA facilities and obtain full access to GSA IT systems.

The contractor shall ensure that roles/privileges assigned to contractor personnel on GSA IT systems are limited to the roles/privileges and information access essential to that individual's performance of his/her assignments. These roles/privileges can be limited or revoked by the Government.

Failure to comply with the contractor personnel security investigative requirements may result in termination of the contract for default.

H.7.1.2 SECURITY AND PRIVACY AWARENESS TRAINING

GSA policy requires contractors to receive security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements. The contractor shall ensure that all contractor personnel performing on this TO complete the following information security training:

a. Annual IT Security Awareness training for contractor initial IT access and annually thereafter; reference NIST 800-53 control AT-2 and GSA Order CIO 2100.3B.
b. Specialized role-based training for contractors that have significant information security responsibilities as defined in the GSA IT security training policy; reference NIST 800-53 control AT-3 and GSA Order CIO 2100.3B when directed.
c. Annual Privacy 101 Training that provides a general awareness of privacy-related issues, laws, privacy protected information, how GSA protects personally identifiable information, and the contractor's role in protecting information; reference Privacy Act of 1974, GSA Order CPO 1878.1, GSA Privacy Act Program, and GSA Order HCO 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information (PII).

H.7.1.3 SECURITY REPORTS

The contractor shall submit a monthly Contractor Access List of all contractor employees that have access to GSA IT systems by the 25th of each month as dictated by Section F. The Contractor Access List shall provide the following information:

a. Contract Employee Name
b. Contractor Company Name
c. GSA Email Address (or other)
d. Task Area and Job Function
e. FISMA System(s) Supported
f. Physical Place of Performance (region/city/state)
g. Facility (contractor, Government, work-at-home)

h. Contract Start Date (EOD)
i. Adjudication Status
j. Adjudication Date
k. Transfer/Termination Dates

Refer to Section J, Attachment K for the Contractor Access List Security Report Template.

H.7.2 INFORMATION ASSURANCE

The contractor may have access to sensitive (to include privileged and confidential) data, information, and materials of the U.S. Government. These printed and electronic documents are for internal use only and remain the sole property of the U.S. Government. Some of these materials are protected by the Privacy Act of 1974 (AMENDED) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

H.7.2.1 SAFEGUARDING SENSITIVE DATA AND INFORMATION TECHNOLOGY RESOURCES

In accordance with FAR 39.105, this section is included in the contract. This section applies to all users of sensitive data and information technology (IT) resources, including awardees, contractors, subcontractors, lessors, suppliers and manufacturers.

The following GSA policies must be followed. These policies can be found at http://www.gsa.gov/directives or https://insite.gsa.gov/directives.

a. CIO P 2100.1 GSA Information Technology (IT) Security Policy
b. CIO P 2100.2B GSA Wireless LAN Security
c. CIO 2100.3B Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities
d. CIO 2104.1A GSA Information Technology IT General Rules of Behavior
e. CIO 2105.1 B GSA Section 508: Managing Electronic and Information Technology for Individuals with Disabilities
f. CIO 2106.1 GSA Social Media Policy
g. CIO 2107.1 Implementation of the Online Resource Reservation Software
h. CIO 2160.4 Provisioning of Information Technology (IT) Devices
i. CIO 2162.1 Digital Signatures
j. CIO P 2165.2 GSA Telecommunications Policy
k. CIO P 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
l. CIO 2182.2 Mandatory Use of Personal Identity Verification (PIV) Credentials
m. CIO P 1878.2A Conducting Privacy Impact Assessments (PIAs) in GSA
n. CIO IL-13-01 Mobile Devices and Applications
o. CIO IL-14-03 Information Technology (IT) Integration Policy
p. HCO 9297.1 GSA Data Release Policy
q. HCO 9297.2B GSA Information Breach Notification Policy

r. ADM P 9732.1 D Suitability and Personnel Security

This section shall be inserted in all subcontracts.

H.7.2.2 SENSITIVE INFORMATION STORAGE

Sensitive data and/or equipment will only be disclosed to authorized personnel on a Need-To-Know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. The contractor's procedures shall be consistent with Government and GSA policies, including GSA Order 2100.1, Information Technology Security Policy (or most current version), Office of Management and Budget (OMB) Memorandums & Circulars, FISMA, the Computer Security Act of 1987, and the Privacy Act.

The disposition of all data will be at the written direction of the COR; this may include documents returned to Government control, destroyed, or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

H.7.2.3 PROTECTION OF INFORMATION

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this TO. The contractor shall also protect all Government data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this contract should be considered as sensitive information. It is anticipated that this information will be gathered, created, and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

H.7.2.4 CONFIDENTIALITY AND NONDISCLOSURE

The contractor shall have all personnel complete a confidentiality agreement prior to performing under this TO. Contractor personnel involved in the management, operation, programming, maintenance, and/or use of IT shall be aware of security responsibilities and fulfill them. Detailed security responsibilities for the contractor are found in the GSA Orders/Handbooks listed in the TOR.

H.7.3 SECURITY CLEARANCES

Positions whose duties require contractors to work with classified national security information (Top Secret, Secret, or Confidential) are national security positions. GSA separates the risk levels for National Security Positions into four categories. The criteria for determining which risk level a particular position falls into is provided in GSA Order ADM 9732.1D – Suitability and Personnel Security Chapter 6, and GSA Order CIO P 2181 – HSPD-12 Personal Identity Verification and Credentialing Handbook.

Contractor personnel assigned to perform onsite data center services at Stennis Space

Center must be U.S. Citizens and possess a final Secret Clearance based on a National Agency Check (NACLC) completed within the last 10 years (in-scope) for unescorted access to the GSA data center hosted at the Stennis Space Center. The clearance must be fully adjudicated at the Secret level and will have an indication of "determined eligibility of Secret" in Joint Personnel Adjudication System (JPAS). Personnel security clearances (PCLs) must be verifiable in the JPAS. All uncleared personnel requiring data center access shall be escorted at all times.

The national security position sensitivity and risk level commensurate with the required level of access for several Network positions is determined Level 3 Critical Sensitive and requires a Top Secret (TS) clearance with Single Scope Background Investigation (SSBI). GSA may require the contractor provide a minimum of two Network Operations personnel in the Washington, D.C. area that are U.S. Citizens and possess a final TS Clearance with Sensitive Compartmented Information (SCI) based on an SSBI completed within the last five years (in-scope). The clearance must be fully adjudicated at the TS level and will have an indication of "determined eligibility of Top Secret" in JPAS. PCLs must be verifiable in JPAS.

H.8 LOGISTICAL SUPPORT PRIVILEGES

For contractor support in Europe, Japan, and Korea, at the discretion of the Military Theatre Commander, the Government may provide, but is not limited to, use of the following:

a. Military or other U.S. Government Clubs, exchanges, or other non-appropriated fund organizations.
b. Military or other U.S. Government commissary stores.
c. Military or other U.S. Government postal facilities.
d. Utilities and services in accordance with priorities, rates, or tariffs established by military or other U.S. Government agencies.
e. Military Payment Certificate, where applicable.
f. Military or other U.S. Government banking facilities.
g. Military or other U.S. Government provided telephones, lines, and services with direct dialing capability and access to the Defense Switched Network (formerly AUTOVON).

The precedence of usage shall be coincident with the urgency of the requirement and in accordance with Government and Military regulations.

H.8.1 OCONUS OPERATIONS

For contractor operations in OCONUS areas, the contractor shall be responsible for adherence to all applicable guidance and agreements. The contractor is responsible for obtaining paperwork and following labor regulations required by foreign governments in order to work OCONUS. The contractor shall comply with all Federal statutes, judicial interpretations and international agreements (e.g., Status of Forces Agreements, Host Nation Support Agreements, etc.) applicable to U.S. Armed Forces or U.S. citizens in the area of operations.. The contractor shall manage and staff the task order with an adequate number of cleared and qualified personnel, approved to work in the various countries, to allow the contractor to perform the required tasks, maintain normal day to day operations, and respond to surge requirements.

The contractor is responsible for obtaining all passports, visas, or other documents necessary to enter and/or exit any area(s) identified by the Task Order and TPOC for contractor employees.

All contractor employees shall be subject to the customs processing procedures, laws, agreements, and duties of the country in which they are deploying to and the procedures, laws, and duties of the U.S. upon re-entry. The contractor is required to register all personnel with the appropriate U.S. Embassy or Consulate.

H.9 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.9.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

In accordance with FAR 2.101(b), if the contractor (and any subcontractors, consultants, or teaming partners) has or is currently providing support or anticipates providing support to GSA IT that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI in accordance with FAR Subpart 9.5. The contractor is also required to complete and sign an Organizational Conflict of Interest Statement in which the contractor (and any subcontractors, consultants, or teaming partners) agrees to disclose information concerning the actual or potential conflict with any proposal for any solicitation relating to any work in the TO. All actual or potential OCI situations shall be identified and addressed in accordance with FAR Subpart 9.5.

H.9.2 NON-DISCLOSURE REQUIREMENTS

The contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) Form (Section J, Attachment F) and ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Are listed on a signed Addendum to Corporate Non-Disclosure Agreement (NDA) Form (Section J, Attachment F) prior to the commencement of any work on the TO,
b. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information, and
c. Are instructed in FAR Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel also must be listed on a signed Addendum to Corporate NDA and be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.14 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 United States Code (U.S.C.) 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all

products and services provided and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

H.16 COST ACCOUNTING SYSTEM

The adequacy of the contractor's accounting system and its associated internal control system, as well as contractor compliance with the Cost Accounting Standards (CAS), affect the quality and validity of the contractor data upon which the Government must rely for its management oversight of the contractor and contract performance. The contractor's cost accounting system shall be adequate during the entire period of performance and shall permit timely development of all necessary cost data in the form required by the contract.

H.18 PURCHASING SYSTEMS

The objective of a contractor purchasing system assessment is to evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting.

Prior to the award of a TO the CO shall verify the validity of the contractor's purchasing system. Thereafter, the contractor is required to certify to the CO no later than 30 calendar days prior to the exercise of any options the validity of their purchasing system. Additionally, if reviews are conducted of the purchasing system after the exercise of the option, the contractor shall provide the results of the review to the CO within 10 workdays from the date the results are known to the contractor.

H.19 EARNED VALUE MANAGEMENT SYSTEM

The contractor shall employ EVM in the management of this TO in accordance with the ANSI/Electronic Industries Alliance (EIA) Standard-748-A-1998, *Earned Value Management Systems.* A copy of the standard is available at http://global.ihs.com/. The Government expects the contractor to employ innovation in its proposed application of EVM techniques to this TO in accordance with best industry practices. The following EVM status information shall be included in each MSR:

a. Planned Value (PV)
b. Earned Value (EV)
c. Actual Cost (AC)
d. A cost curve graph plotting PV, EV, and AC on a monthly basis from inception of the TO through the last report, and plotting the AC curve to the estimated cost at completion (EAC) value.
e. An EVM variance analysis that includes the following:
    1. Cost variance (CV) = (EV - AC)
    2. Cost Variance % = (CV/PV X 100%)
    3. Cost Performance Index (CPI) = (EV/AC)
    4. Schedule Variance = (EV minus PV)

5. Schedule Variance % = (SV/PV X 100%)
6. Schedule Performance Index (SPI) = (EV/PV)
7. Estimate at Completion (EAC)
8. AC Cumulative (cum) + 1/CPI X (Baseline at Complete (BAC) minus EV cum)
9. AC cum + 1/CPI X SPI X (BAC minus EVcum)
10. Variance at Completion (VAC) = (BAC minus EAC) for EAC
11. Variance at Completion % + (VAC/BAC X 100%) for EAC
12. Estimate to Completion (ETC)
13. Expected Completion Date

f. Explain all variances greater than 10 percent.
g. Explain, based on work accomplished as of the date of the report, whether the performance goals will be achieved.
h. Discuss the corrective actions that will be taken to correct the variances, the risk associated with the actions.

The Government will conduct an Integrated Baseline Review within 150 calendar days after PS, or exercise of significant TO options, or incorporation of major TO modifications. The objective of the Integrated Baseline Review is for the Government and the contractor to jointly assess areas, such as the contractor's planning, to ensure complete coverage of the TO, logical scheduling of the work activities, adequate resources, and identification of inherent risks. EVM will be applied to projects selectively and at varied levels under performance of this TO.

H.23 TRAVEL

The contractor will be required to travel to CONUS and OCONUS locations to include after hours and weekends in performance of this TO.

The contractor must provide their own vehicles for local travel. The Government will not reimburse for local travel or provide Gov't furnished vehicles.

The contractor shall enroll in RAPIDgate http://www.rapidgate.com/ to facilitate the delivery of services to customers on military or other DoD installations.

H.23.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. FTR - prescribed by the GSA, for travel in the contiguous U.S.
b. JJTR, Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

H.23.2 TRAVEL AUTHORIZATION REQUESTS

Before undertaking travel to any Government site or any other site in performance of this Contract, the contractor shall have this travel approved by, and coordinated with, the FEDSIM COR and TPOC. Notification shall include, at a minimum: the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the contractor shall prepare a Travel Authorization Request for Government review and approval. Long distance travel will be reimbursed for cost of travel comparable with the FTR, JTR, and DSSR.

Requests for travel approval shall:

a. Be prepared in a legible manner.
b. Include a description of the travel proposed including a statement as to purpose.
c. Be summarized by traveler.
d. Identify the TO number.
e. Identify the CLIN associated with the travel.
f. Be submitted in advance of the travel with sufficient time (10 days) to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.24 ODCs

The Government may require the contractor to purchase hardware, software, cloud services, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified at the time a TOR is issued or may be identified during the course of a TO by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO and the prime contractor has an approved purchasing system, the contractor shall submit to the FEDSIM COR a Request to Initiate Purchase (RIP). The RIP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the COR without complying with the requirements of Section H.25, Commercial Software Agreements.

H.25 COMMERCIAL SOFTWARE AGREEMENTS

H.25.1 The Government understands that commercial software tools that may be purchased in furtherance of this TO as described in Section C.5 and as contemplated in the Tools and ODC CLINs in Section B may be subject to commercial agreements which may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic or online format such as "clickwrap" or "browsewrap" (collectively, "Software Agreements"). The parties acknowledge that the FAR clause at 12.212(a) requires the Government to procure such tools and their associated documentation under such Software Agreements to the extent such Software Agreements are consistent with Federal law.

H.25.2 In order to ensure that the Software Agreements are consistent with Federal law, the contractor shall not make any purchase contemplated in Section C.5 above without first securing

the consent of the licensor of such software tools to amend the Software Agreements in accordance with the Amendment clause set forth in Section H.25.4 below. The contractor shall submit documentary evidence of such consent as part of its technical proposal.

H.25.3 The requirements of this Section H.25.3 apply only to those commercial software tools newly purchased under this TO; they do not apply to software furnished as GFI/GFE (if any). Further, they apply only to those Software Agreements that define the Government as the licensee or are intended to be transferred or assigned to the Government, with the Government becoming the licensee, at the end of this TO.

H.25.4 As used in the Amendment clause, the term "this Agreement" refers to each Software Agreement. The relevant definitions and the capitalization of terms (e.g., Licensee, Licensor, Software, and Agreement) may be adjusted as necessary to match the nomenclature of the Software Agreement.

Amendment

For Federal Government Licensees, this Agreement is hereby amended as follows:

1. ***Dispute resolution and governing law****:* Any arbitration, mediation or similar dispute resolution provision in this Agreement is hereby deleted. This Agreement shall be governed by and interpreted and enforced in accordance with the laws of the United States of America, and dispute resolution shall take place in a forum, and within the time period, prescribed by applicable federal law. To the extent permitted by federal law and then only to the extent not preempted by federal law, the laws of the state specified in this Agreement (excluding its choice of law rules) will apply. No equitable or injunctive relief, and no shifting of legal fees or costs, may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.
2. ***Indemnification***: Any provisions in this Agreement requiring any Federal Government Licensee to indemnify any party are hereby deleted and shall not apply. Any provisions requiring the licensor to indemnify the Federal Government Licensee shall be revised to state that such indemnification, and the conduct and/or settlement of any applicable proceedings, shall be subject to 28 USC 516.
3. ***Changes in templates***: This Agreement shall apply in the version attached hereto. Subsequent updates to or changes in the licensor's standard commercial templates for such agreements shall not be binding on the Federal Government Licensee, except by prior express written agreement of both parties.
4. ***Fees, taxes and payment:*** If the Software is licensed as part of a separate Government contract between the Federal Government Licensee and a prime contractor, the provisions of such contract regarding fees, taxes and payment shall supersede any provisions of this Agreement regarding same. Notwithstanding the foregoing: (a) express written agreement of the Federal Government Licensee shall be required prior to (i) any extension or renewal of this Agreement or the associated fees or (ii) any change in the fees; (b) late payments shall be governed by the Prompt Payment Act and the regulations at 5 CFR 1315; and (c) no cost of collection on delinquent invoices may be sought

against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.

5. ***Assignment*:** Licensor may not assign this Agreement or its rights or obligations thereunder, in whole or in part, except in accordance with the procedures set forth in FAR subparts 32.8 and/or 42.12, as applicable.
6. ***No waiver of liability or cause of action***: Any provision requiring the Federal Government Licensee to agree to waive or otherwise not to pursue any claim against the licensor it may otherwise have is hereby deleted. Without limiting the generality of the foregoing, the parties agree that nothing in this Agreement, including but not limited to the limitation of liability clauses, in any way grants the licensor a waiver from, release of, or limitation of liability pertaining to, any past, current or future violation of federal law and that no clause restricting users' statements shall be read to restrict the Federal Government Licensee's ability to pursue any course of action otherwise permitted by federal law, regulation, or policy, including without limitation making public statements in connection with any suspension or debarment action.
7. ***Audit***: Any clauses in this Agreement allowing for an audit of the Federal Government Licensee's records or information systems, or verification of its compliance with this Agreement generally, shall be subject to the Federal Government Licensee's requirements pertaining to security matters, including without limitation clearances to be held and non-disclosure agreements to be executed by auditors, badging or escorting requirements for access to premises, and other applicable requirements. Any overuse identified in an audit shall be referred to the prime contractor or the Federal Government Licensee's contracting officer (as applicable) for action. No audit costs may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.
8. ***Compliance with laws*:** The parties acknowledge that the U.S., as a sovereign, is subject to the laws of the U.S. Nothing in this Agreement shall be interpreted to imply consent by any Federal Government Licensee to submit to the adjudicative or enforcement power of any regulatory, administrative, or judicial authority of, or the application of the laws of, another jurisdiction. Any provision inconsistent with applicable federal law that is not listed above is hereby deemed omitted from this Agreement to the extent of such inconsistence.
9. ***Third party terms***: Any third party licensing terms associated with third-party software components or products embedded in or otherwise provided with the Software shall be deemed amended in accordance with sections 1-8 above.

H.26 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14 apply. The Software Agreements referenced in Section H.25, amended as contemplated therein, shall be deemed to constitute such disclosure with regard to their associated commercial software tools and shall prevail over any inconsistent provision in FAR 52.227-14 to the extent of such inconsistency.

H.27 AWARD FEE

See the Draft AFDP in Section J, Attachment G.

H.28 SMALL BUSINESS UTILIZATION

Per FAR 52.219-8, Utilization of Small Business Concerns, the Government is committed to ensuring that small businesses are provided maximum practicable opportunity to participate as subcontractors in the performance of this TO.

The contractor shall report the percentage of subcontracted dollars allocated for small business subcontract support. The contractor shall submit a report with this information according to Section F.

I.2.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request the CO will make their full text available. Also, the full text of a provision may be accessed electronically at:

FAR website: http://www.acquisition.gov/far/

Clause No	Clause Title	Date
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	(Apr 2014)
52.204-2	Security Requirements	(Aug 1996)
52.204-7 (Provision)	System for Award Management	(Jul 2013)
52.204-9	Personal Identity Verification of Contractor Personnel	(Jan 2011)
52.204-13	System for Award Management Maintenance	(Jul 2013)
52.204-14	Service Contract Reporting Requirements	(Jan 2014)
52.215-21	Requirements for Cost or Pricing Data or Information Other than Cost or Pricing Data – Modifications	(Oct 2010)
52.215-22	Limitations on Pass-Through Charges- Identification of Subcontractor Effort	(Oct 2009)
52.215-23	Limitations on Pass-Through Charges	(Oct 2009)
52.216-7	Allowable Cost and Payment Fill-in: 30th	(Jun 2013)
52.217-5 (Provision)	Evaluation of Options	(Jul 1990)
52.217-8	Option to Extend Services Fill-in: 30 days	(Nov 1999)
52.219-8	Utilization of Small Business Concerns	(Jul 2013)
52.223-13	Acquisition of EPEAT Registered Imaging Equipment	(Jun 2014)
52.223-15	Energy Efficiency in Energy-Consuming Products	(Dec 2007)
52.223-16	Acquisition of EPEAT-Registered Personal Computer Products	(Jun 2014)
52.224-1	Privacy Act Notification	(Apr 1984)
52.224-2	Privacy Act	(Apr 1984)
52.225-13	Restrictions on Certain Foreign Purchases	(Jun 2008)
52.227-14	Rights in Data – General	(Dec 2007)
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	(Dec 2007)
52.227-17	Rights In Data Special Works	(Dec 2007)

Clause No	Clause Title	Date
52.232-18	Availability of Funds	(Apr 1984)
52.232-20	Limitation of Cost	(Apr 1984)
52.232-22	Limitation of Funds	(Apr 1984)
52.232-99	Providing Accelerated Payment to Small Business Subcontractors (Deviation)	(Aug 2012)
52.237-3	Continuity of Services	(Jan 1991)
52.239-1	Privacy or Security Safeguards	(Aug 1996)
52.243-7	Notification of Changes Fill-in: 10 **business** days	(Apr 1984)
52.244-6	Subcontracts for Commercial Items	(Dec 2013)
52.246-5	Inspection of Services—Cost-Reimbursement	
52.246-25	Limitation of Liability – Services	(Feb 1997)
52.247-14	Contractor Responsibility for Receipt of Shipment	(Apr 1984)
52.247-67	Submission of Transportation Documents for Audit Fill-in: COR, see Section G	(Feb 2006)
52.249-6	Termination (Cost-Reimbursement)	(May 2004)
52.249-14	Excusable Delays	(Apr 1984)
52.251-1	Government Supply Sources	(Aug 2012)

I.2.2 FULL TEXT CLAUSES

FAR 52.217-9: OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 10 days provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five years and six months.

I.4 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at:

GSAM website: https://www.acquisition.gov/gsam/gsam.html

Clause No	Clause Title	Date
552.204-9	Personal Identity Verification Requirements	(Oct 2012)
552.232.25	Prompt Payment	(Nov 2009)
552.236-75	Use of Premises	(Apr 1984)
552.239-70 (Provision)	Information Technology Security Plan and Security Authorization	(Jun 2011)
552.239-71	Security Requirements for Unclassified Information Technology Resources	(Jan 2012)

J.1 LIST OF ATTACHMENTS

Attachment	Title
A	COR Appointment Letter
B	Monthly Status Report
C	Department of Defense (DD) 254
D	Travel Authorization Template
E	Request to Initiate Purchase Template
F	Corporate Non-Disclosure Agreement
G	Award Fee Determination Plan
H	Acronym List
I	Problem Notification Report
J	Deliverable Acceptance-Rejection Report
K	Contractor Access List Template
L	GSA Customer Locations
M	GSA IT Information Resource Management (IRM) Strategic Plan
N	GEO External IT Support List
O	Deskside Support ROB Hours of Coverage Per GSA Region
P	RESERVED
Q	RESERVED
R	RESERVED
S	Incremental Funding Table Award (electronically attached)
T	RESERVED
U	RESERVED
V	RESERVED
W	RESERVED

This page intentionally left blank.